ATLANTIS PRESS
Atlantis Highlights in Computer Sciences, volume 3
21st International Scientific Workshop on Computer Science and Information Technologies (CSIT 2019)

Information Security Risk Assessment Methodology and Software "Rubikon"

Olga Vybornova
Department of Information Security
Astrakhan State University
Astrakhan, Russia
olga.vyb.90@gmail.com

Igor Pidchenko
Department of Information Security
Astrakhan State Technical University
Astrakhan, Russia
igor.pidchenko@gmail.com

Iskandar Azhmukhamedov
Department of Information Security
Astrakhan State University
Astrakhan, Russia
iskander_agm@mail.ru

***Abstract*—Risk assessment is an important part of the process of ensuring the required levels of information security of an organization. An urgent task is to develop a methodology for assessing information security risks, allowing not only to assess risks at the asset level, but also to trace their impact on the organization's activities. This article describes the methodology of information security risk assessment "Rubikon", including the algorithm of the acceptable risk assessment, fuzzy cognitive model and the algorithm of the current risks assessment. To determine the level of acceptable risk, we proposed to construct an acceptable risk curve. The developed model and the algorithm of the current risks assessment allow determining the set of values characterizing the current level of information security risks based on establishing of relationships between negative events, potential threats, protective measures, implemented attacks, information assets, sub-processes and main business processes of the organization. Results visualization is a set of points on the "damage-probability" coordinate plane. The conclusion about the acceptability of risks is made based on an analysis of the location of these points relative to the acceptable risk curve. In order to reduce the complexity of the risk assessment procedure using the «Rubikon» methodology manually, we developed software. In addition, the article provides an example of risk assessment using this software and a comparison of the results with the proven method. This proves the adequacy and reliability of the proposed approach to information security risk assessment.**

Keywords—information security, risk assessment, subjective uncertainty, fuzzy cognitive model, acceptable risk, current risk, Rubikon, risk assessment software

I. INTRODUCTION

Any activity other than material and energy flows includes an informational component. At the same time, risk management properties violation information (confidentiality, integrity, availability, etc.) during its processing plays an important role in ensuring the reliable operation of information processing processes and achieving the required level of information security [1].

Risk assessment is a tool for risk management and is a method of identifying vulnerabilities and threats, assessing possible impacts. It allows you to select adequate protective measures for those systems and processes in which they are necessary. Risk assessment allows you to make security cost-effective, relevant, timely and able to respond to threats [2].

The need for risk assessment is defined in Russian and international standards for information security [3-5] and regulatory documents of state bodies of the Russian Federation (the FSTEC's of Russia documents on the protection of personal data and key information infrastructure systems) [6]. Currently there are a large number of works by Russian and foreign scientists devoted to the problem of information security risk management [7-10]. However, risk assessment in them is conducted only to the level of assets; their impact on the functioning of the organization is not taken into account. Consequently, the obtained values are not sufficiently informative, which does not allow the decision maker to make an informed choice of management decisions.

In this regard, an urgent task is to develop a methodology for assessing information security risks, allowing not only to assess risks at the asset level, but also to trace their impact on the organization's activities. In addition, it is necessary to take into account the presence of subjective uncertainty associated with the participation of experts. It is the purpose of this work.

II. DEVELOPMENT OF METHODOLOGY

We developed an information security risk assessment methodology "Rubikon", based on expert information. It includes the following steps:

1. Assessment of acceptable risk by constructing an acceptable risk curve.
2. Assessment of current (actual) risks by applying fuzzy cognitive modeling (FCM) methodology.
3. Analysis of the results (visualization, the comparison of values describing the current state of the system with values of risks acceptable for the decision maker).

Let us consider in more detail the steps of the methodologyy.

A. Assessment of acceptable risk

Acceptable risk – is the risk that the decision maker is prepared to accept in the present situation. To determine its level, we proposed to take into consideration the functional dependence of the probability of damage occurrence on its value, which is reflected in the acceptable risk curve (ARC).

The algorithm for constructing an acceptable risk curve includes the following main steps [11]:

1. Experts classify the damage (U_i) that could potentially be caused by the negative event (NE) to assets of the organization. In this case, they usually

use the verbal form to describe the categories of damage. To compare the numerical estimates of various classes of damage, it is advisable to use the Harrington scale [12] and determine each category of damage as a fraction of the critical damage (U^{cr}): "*Damage is insignificant*" – $0{,}1 \cdot U^{cr}$; "*Damage is of little significance*" – $0{,}29 \cdot U^{cr}$; "*Damage is of medium significance*" – $0{,}51 \cdot U^{cr}$; "*Damage is significant*" – $0{,}72 \cdot U^{cr}$; «*Damage is critical*» – $1 \cdot U^{cr}$. However, the expert can also choose the necessary number of reference values for constructing a curve.

2. The decision maker assesses the probability (P_i^*) of occurrence of various categories of damage (U_i) in terms of their acceptability. The result is a set of points $R^* = \{(U_i; P_i^*)\}_{i=1..N}$.
3. The values of P_i^*, specified at the reference points U_i, are approximated by a continuous function of the form:

$$P^* = a \cdot \exp(-b \cdot (U - U^{is})), \quad (1)$$

where a and b – some constants: a – corresponds to the probability with which the occurrence of insignificant damage is allowed U^{is}; b – determines the speed of the fall of the acceptable probability of taking damage as it approaches the critical damage U^{cr} (Fig. 1).

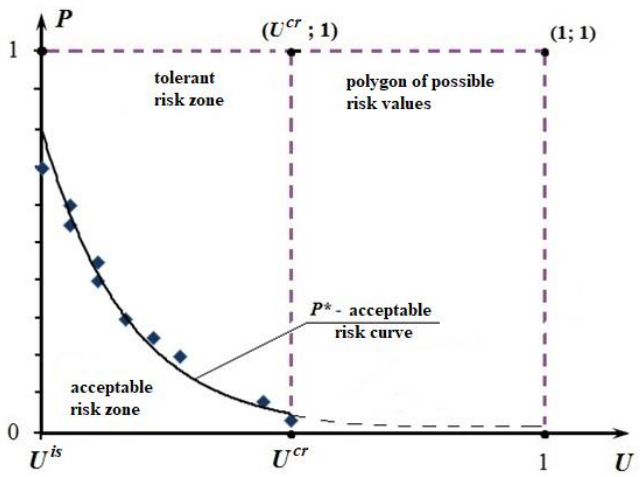

Fig. 1. Acceptable risk cupve

The area bounded by the coordinate axes and the ARC is called the acceptable risk zone. The tolerant risk zone shows the maximum level of risk that an organization can withstand without significant damage to its financial and competitive position.

B. Assessment of current risks

To assess current information security risks within the framework of fuzzy cognitive modeling methodology [13-14] we formulated a FCM, represented by a tuple:

$$RSK = \langle G, QL, \{\alpha_{ij}\}, R, Def \rangle,$$

where:

- G – fuzzy cognitive graph;
- QL = {*Low* (*L*); *Below-Average* (*BA*); *Average*. (*A*); *Above-Average* (*AA*); *High* (*H*)} – term-set of linguistic estimates of the parameters of the graph, which is associated with a fuzzy classifier, containing trapezoid numbers (a_1, a_2, a_3, a_4), where a_1 and a_4 (a_2 and a_3) – coordinates of the lower (upper) base of the trapezium: {«*L*» (0; 0; 0,15; 0,25); «*BA*» (0,15; 0,25; 0,35; 0,45); «*A*» (0,35; 0,45; 0,55; 0,65); «*AA*» (0,55; 0,65; 0,75; 0,85); «*H*» (0,75; 0,85; 1; 1)};
- $\{\alpha_{ij}\}$ – set of weights of edges of the graph G;
- R – the set of rules for the aggregation of the influence of various low-level concepts on the top-level concept;
- $Def\ (A) = (a_2 + a_3) / 2$ – function defuzzification fuzzy trapezoidal values A (a_1, a_2, a_3, a_4), obtained as a result of computations by FCM [15].

The graph G includes the following levels: lower, 7th – negative events (NE); 6th – threats to information assets, posed by NE; 5th – protective measures (PM); 4th – attacks (threats, that have passed through the PM); 3rd – risks to information assets (IA) (probable deterioration of the organization's assets); 2nd – risks to subprocesses (SP); 1st – risks to main processes (MP) of organization (probable malfunction of MP); 0th – information security risks to the organization as whole (Fig. 2).

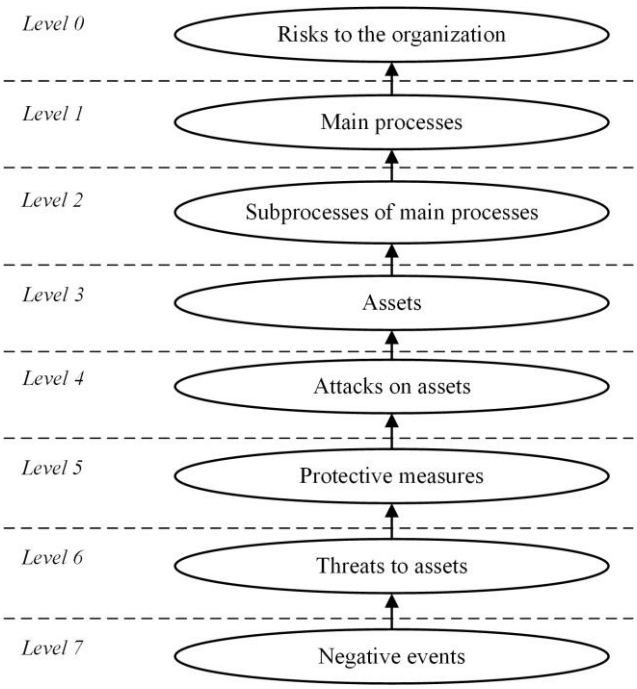

Fig. 2. Levels of the FCM's graph of current risk assessment

The algorithm for assessing current information security risks includes the following steps:

First stage – Formation of a risk assessment FCM:

1. Identification of main processes of the organization.
2. Identification (if necessary) of sub-processes of main processes.
3. Identification of information assets supporting the operation of sub-processes.

Second stage – Risk calculation:

4. Determining the set of potentially possible NE and assessment of probabilities of their occurrence.
5. Determining the threats, that can be generated by NE. Estimation of the intensities of these threats I_i and the probabilities of their occurrence P_i. In this case, intensity refers to potential damage that may be caused by a threat.
6. Evaluation of the effectiveness of the impact of protective measures on the intensity Z_{I_i} and probability Z_{P_i} of the threat.
7. Calculation of residual (after protective measures) probabilities of attacks (P_{Att_P}) on information assets and their damage (U_{Att_I}):

$$P_{Att\,i} = P_i \cdot \left(1 - Z_{P_i}\right), \tag{2}$$

$$U_{Att\,i} = I_i \cdot \left(1 - Z_{I_i}\right), \tag{3}$$

8. The calculation for each SP, based on the values obtained by the formula (3) in step 7, the damage by the formula:

$$U_i^{k,j} = \alpha_i^{k,j} U_i^{k+1,j}, \tag{4}$$

where $U_i^{k,j}$ – i-th damage to j-th concept of k-th level of FCM $\alpha_i^{k,j}$ – weighting factor, reflecting the impact of i-th damage of (k+1)-th level concept to j-th concept of k-th level of FCM; $U_i^{k+1,j}$ – damage caused to i-th concept of (k+1)-th level of FCM, influencing to j-th concept of k-th level; $k \in \{0; 1; 2\}$.

9. Determination by the formula (4) with $k = 1$ damage to main processes. In this case, at stages 8 and 9, the probabilities of attacks remain unchanged (calculated at step 7 using formula (2)).
10. Calculation of information risks of the organization using the formula (4) with $k = 0$.

As a result of risk assessment, we get the set of values $R_{cur} = \{(U_i; P_i)\}$, that characterize the current indicators of information security risks for the organization in general, where $i = 1...N$; N – the number of possible damage values. These values are made by dots on the "damage-probability" coordinate plane, where the acceptable risk curve is already constructed (1). If some information assets are involved in more than one MP, the risks for the IA are re-accounted for taking into account their weights in the MP (in this case, any threat of this kind on the "damage-probability" coordinate plane corresponds to more than one point). An example of current risk assessment results is shown in Fig. 3.

Above the acceptable risk curve are points that characterize unacceptable risk values (for example, point A_0 in Fig. 3). For them it is necessary to apply measures to reduce to an acceptable level. For points located below the acceptable risk curve (for example, point A_1 in Fig. 3), the risk is acceptable, additional protection is not required.

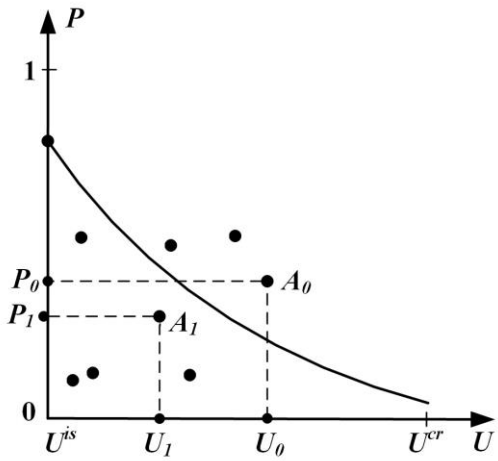

Fig. 3. Current risk assessment results

III. Information Security Risk Assessment Software "Rubikon"

The proposed methodology involves working with fuzzy trapezoid numbers, as well as the need to monitor the relationship between the elements of the risk assessment model. In order to reduce the complexity of the risk assessment procedure using the «Rubikon» methodology manually, we developed software. Risk assessment is based on the establishment of relationships between negative events, potential threats, protective measures, implemented attacks, information assets, sub-processes and main business processes of the organization (Fig. 4).

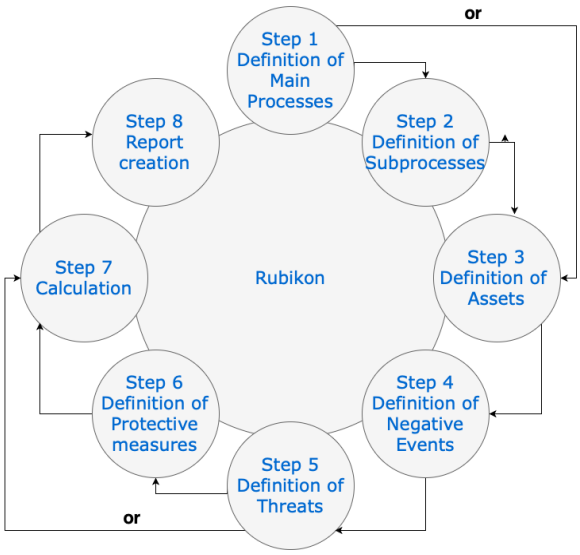

Fig. 4. "Rubikon" methodology algorithm

The software allows you to create an assessment project, assess risks, save the assessment results as a file and load a previously saved project. As a result of the software's work, the magnitude of the current information security risks in the form of a set {(damage, probability)} is calculated, and also compared with acceptable values for the organization with a view to further management decisions.

The C++ language was chosen as a tool for software implementation using the Qt Framework. This Framework allows you to implement a graphical user interface: create and manage windows, process system messages and commands from input devices (keyboard, mouse, etc.). .

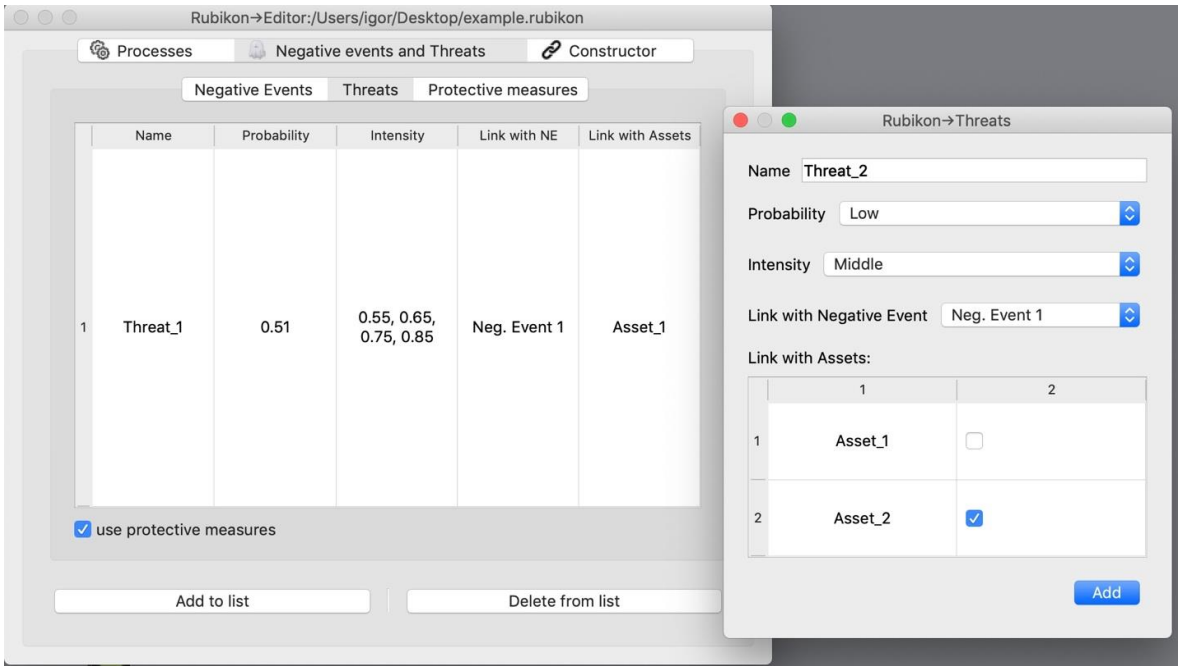

Fig. 5. "Rubikon" software interface

In addition, the choice of this tool was due to the possibility of cross-platform implementation of software without the need for a serious software upgrade. At the same time, Qt is open source software that allows you to extract commercial benefits from a software product while observing the GPL / LGPL license [16].

In developing the program, the methodology of object-oriented programming (OOP) was used. When designing the user interface of the software (Fig. 5), emphasis was placed on the maximum simplification of the risk analysis procedure. We designed 16 classes and 12 graphic formsFig. 6 shows the database structure.

The "Rubikon" software project is a SQLite 3 database [17]. This choice is due to the fact that the "Rubikon" methodology implies the existence of logical links with all the elements that are added by the user. Considering that, there may be many elements, and if elements are deleted or changed, logical links may also change, the use of the database is the most effective way to interact with the methodology. In «Rubikon» software, all changes are made while working on a project are recorded in a SQLite transaction, and upon completion of work, the user will be able to save changes or discard them.

IV. Example of Risk Assessment

Using the developed methodology "Rubikon", we performed an information security risk assessment in a number of Astrakhan organizations. Based on the results of the assessment, we proposed measures to reduce unacceptable risks to an acceptable level. For example, an information security risk assessment was carried out for the main process "Information Resources Management" of the Astrakhan University. This process associated with the maintenance of efficiency of the automated information system of the University, as well as ensuring an appropriate level of information security of university information systems. The expert group formed a set of threats, constructed the FCM for assessing current risks and made calculations. To build a fuzzy cognitive model, a description of this process was used in the university's quality management system. Some results of risk assessment are shown in Fig. 7. Damage indices are marked on the abscissa axis; probability on the ordinate axis. As we can see, some risks are unacceptable. For them it is necessary to choose protective measures.

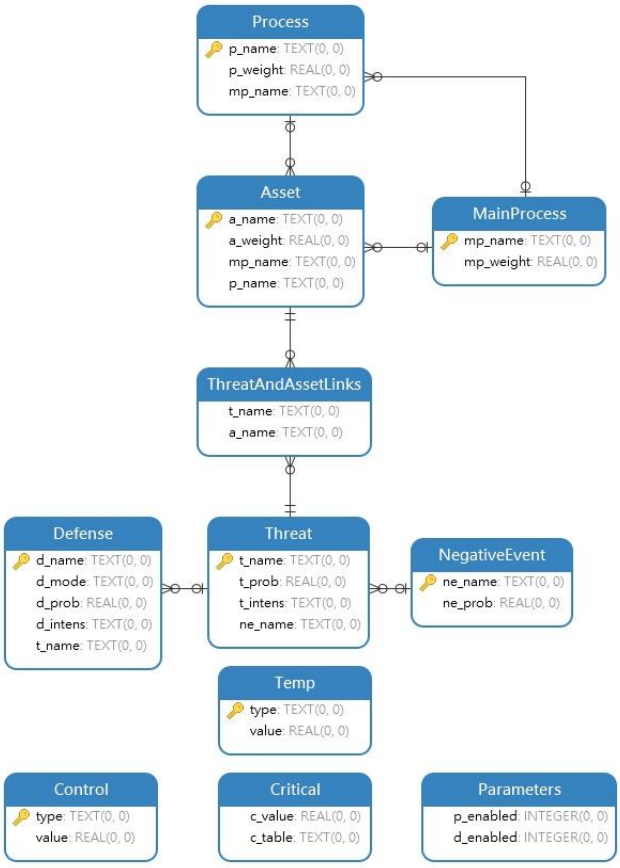

Fig. 6. "Rubikon" project file's database structure

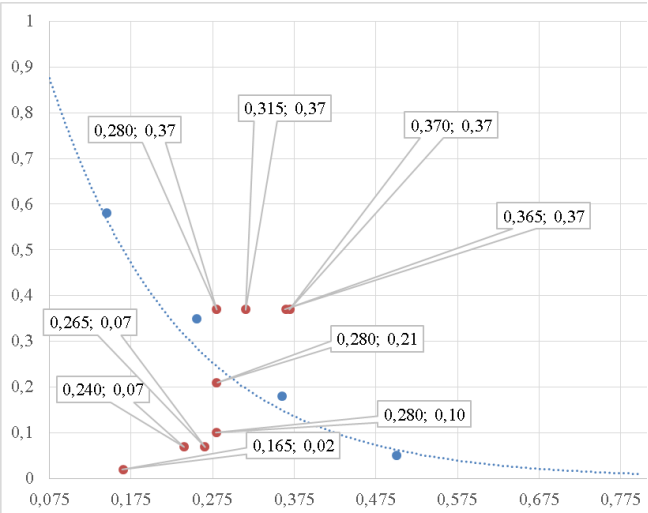

Fig. 7. Some results of risk assessment for the process "Information Resources Management"

In order to validate the results obtained with the methodology "Rubikon", the information security risk assessment was carried out based on similar initial data, using the vsRisk method [18]. We chose this method because, on the one hand, it is widely used, and on the other hand, the input data for risk assessment using vsRisk are the same parameters that are used in the methodology "Rubikon". This ensures correct comparison of results. Table 1 presents a summary of risk acceptability, obtained using the methods of "Rubicon" and "vsRisk".

TABLE I. COMPARISON OF RISK ASSESSMENT RESULTS

Threat	Status of risk	
	"Rubikon"	***"vsRisk"***
Destruction of network and technological equipment	unacceptable	unacceptable
Getting control of network and technological equipment	unacceptable	unacceptable
The threat of disabling database server	acceptable	acceptable
The introduction of malicious code to the database server	unacceptable	unacceptable
Theft of system documentation	acceptable	acceptable
The threat of disabling staff	acceptable	acceptable
Theft of application and system software (physical unauthorized access)	acceptable	acceptable
Copy or theft of application and network software (by LAN)	unacceptable	unacceptable
Theft of technological and network equipment	acceptable	unacceptable

Comparison of the results showed a high level of consistency of values, which confirms the accuracy and validity of the proposed risk assessment methodology [15]. The difference in the risk status of the threat "Theft of the technological and network equipment" is not significant, since according to the results of the "Rubikon" assessment, it is close to the acceptable risk curve (the point (0.28; 0.21) in Fig. 7). However, the use of vsRisk does not allow decision makers to take well-founded decisions on risk management, since this method does not take into account the relationship of assets with the main processes of the organization, in contrast to the approach proposed in this paper.

V. CONCLUSION

The developed methodology "Rubikon" allows for information security risks assessment in conditions of subjective uncertainty. The values, obtained from the assessment results, are noted on the "damage-probability" coordinate plane, which increases the visibility of the results for decision makers. The software automates the risk assessment procedure, thereby facilitating the application of the methodology in practice. The adequacy and accuracy of the proposed approach to risk assessment is confirmed by the correct application of the mathematical apparatus, as well as consistency with the available scientific results. This methodology and software can be used together with the threat data bank formed by the FSTEC of Russia [19], as well as basic typical models of information security threats in the information systems of various classes and types, developed by the FSTEC of Russia [6]. A certificate of state registration of computer programs has been received for the software implementing the proposed methodology [20].

REFERENCES

[1] "Why Information Risk is a Board-level Issue". http://www.iaac.org.uk/media/1066/why-information-risk.pdf.

[2] S. V. Zawoyski, K. Hooper, M. J. Chagares, "How to achieve excellent enterprise risk management. Why risk assessment fail". https://www.pwc.ch/de/publications/2016/pwc_excellent_enterprise_risk_management_e.pdf.

[3] ISO/IEC 27001:2013 "Information technology – Security techniques – Information security management systems – Requirements", 2013.

[4] "Enterprise Risk Management – Integrated Framework": Executive summary. COSO, 2004. http://www.coso.org/ERM-IntegratedFramework.htm.

[5] RS BR IBBS-2.2-2009 "Methodology for risk assessment of information security breaches". Moscow, 2009 (In Russian).

[6] "Methodology for determining information security threats in information systems": methodological document of the FSTEC of Russia (draft) of May 7, 2015. – http://fstec.ru/component/attachments/ download/812 (In Russian).

[7] I. V. Anikin, "Information Security Risks Assessment Method Based on AHP and Fuzzy Sets". In: *Proc. of 2nd Intl' Conference on Advanced in Engineering Sciences and Applied Mathematics (ICAESAM'2014)*. Istambul (Turkey), 2014, pp. 11-15.

[8] I. V. Isaev, "IT risks and information security". *Modern high technologies*. 2014, No. 7 (part 1), pp. 184-184. http://www.top-technologies.ru/ru/article/ view?id=34276 (In Russian).

[9] B. Evans, "Key Components of a High-Performing Information Risk Management Program", 2015. https://securityintelligence.com/key-components-of-a-high-performing-information-risk-management-program/.

[10] G. Jenkins, "Information security framework programme": Risk methodology, 2014. http://sites.cardiff.ac.uk/isf/files/2014/05/ISFRiskAssessmentMethodologyv1_ 2.pdf.

[11] I. M. Azhmukhamedov, O. N. Vybornova, Yu. M. Brumshtein, "Management of Information Security Risks in a Context of Uncertainty". *Automatic Control and Computer Sciences*. 2016. Vol. 50, No. 8, pp. 657–663. – DOI: 10.3103/S0146411616080022

[12] E. C. Harrington, "The desirable function". *Industrial Quality Control*. 1965, V. 21, No. 10, pp. 494-498.

[13] Z. K. Avdeeva, S. V. Kovrigina, D. I. Makarenko, "Cognitive modeling to solve semistructured systems management tasks". M.: Inst. Of Contr. Sc. of Rus. Acad. of Sc., 2006, pp. 41–54 (In Russian).

[14] I. M. Azhmuhamedov, "Dynamic Model of the Impact of Threats to Information Security System". *IT Security*. 2010, Vol. 17, no. 2, pp. 68-72 (In Russian).

[15] O. N. Vybornova, "Information processing risk management based on expert assessments": abstr. diss. cand. tech. sc., Astrakhan, 2017 (In Russian).

[16] QT Documentation. https://doc.qt.io/.

[17] SQLite Documentation. https://www.sqlite.org/ docs.html.

[18] vsRisk. http://www.vigilantsoftware.co.uk/t-trial.aspx.

[19] Information Security Threat Data Bank. http://bdu.fstec.ru/ (In Russian).

[20] O. N. Vybornova, I. A. Pidchenko, I. M. Azhmuhamedov "Information security risk assessment system Rubikon": software. Cert. of state reg. of comp. program. No. 2018666853. 21.12.2018 (In Russian).