ANNOTATION

of the dissertation work of doctoral student PhD
on the specialty 6D070400 - «Computer technology and software»
Zhekambayeva M.N.
on the theme «Methods for analysis and evaluation of the the security risks of information resources »

The relevance of the research theme. The rapid development of the IT infrastructure of the enterprises leads to an uncontrolled increase in the amount of threats and vulnerabilities of information resources (IR). In these conditions, risk analysis and evaluation is required for the creating a risk control and information security (IS) management system for the protection object.

Nowadays, there are many risk analysis and evaluation means (RAEM), from regulatory documents (standards) till the specific software applications. Choosing them for practical use the expert faces many questions such as "What parameters should be used?", "What mathematical apparatus should I use?", "How to evaluate without statistical data?", "How to analyze and evaluate the risks in an uncertain conditions?" etc. These and other factors create a number of difficulties at the selection of appropriate means of evaluation.

It should also be noted that statistical data about IS incidents and threats are used mainly for risk analysis and evaluation. In many countries, including Kazakhstan, there is no corresponding state policy regarding the registration and application of such statistics. This limits the capacity of existing RAEM for national use. In addition, such means have certain limitations on the used set of parameters that lead to a decrease of their flexibility; it does not allow their use in evaluation of a wider range of values. Also, there are not enough studied the problems of the expert evaluation formation, made in a fuzzy defined, poorly formalized environment, taking into account the period of time, the economic specifics of the enterprise and other factors.

Therefore, it is necessary to develop and investigate methods and means that allow to create more flexible in the use RAEM of IS both on the basis of statistical data and on the basis of expert evaluation, made in a fuzzy defined, poorly formalized environment, that determines ***the relevance of the theme of the scientific research and its purpose***.

The main tasks of the research:

1. To analyze and investigate the basic notions related to risk, existing standards, methods, methodologies and RAEM software, with the aim of defining a set of basic characteristics used for the creation and selection of the most effective tool for solving the relevant IP tasks;
2. On the basis of the obtained basic characteristics to develop a tuple model of the basic characteristics of the RTM, which allow dynamically to determine the sets of values and thus to ensure the flexibility of the corresponding developed RAEM of IS;

3. On the basis of the proposed RTM model to develop methods for IS risks analysis and evaluation, that will allow creating effective evaluation tools that use as an input data the dynamically variable sets of deterministic and fuzzy defined basic characteristics;

4. To develop methods that will allow equivalently to redefine the order (the number of terms) of a linguistic variable (LV) based on the standard parametric trapezoidal fuzzy numbers (FN) with *n*-fold incrementing at solving problems of IS risks analysis and evaluation.

5. Using the proposed methods and models to develop a methodology for the synthesis of systems of IS risks analysis and evaluation, allowing to formalize and generalize the process of creation both software and hardware systems designed for effective risks evaluation;

6. On the basis of the proposed methods, models and methodologies, to develop new structural solutions of the systems in the field of information risk analysis;

7. On the basis of the proposed methodology and structural diagrams of the corresponding systems to develop software of RAEM and carry out its experimental study in order to verify the developed methods, models and structural solutions.

The object of the research - the process of IS risks analysis and evaluation;

The subject of the research - models, methods, systems, methodologies and software tools for risks analysis and evaluation in the field of information security.

Methods of the research. The conducted researches are based on modern methods of fuzzy logic theory (development of methods for risks analysis and evaluation, as well as methods of *n*-fold incrementing of the number of terms of linguistic variables), decision-making, algorithms, object-oriented programming (development of RAEM IS software), modeling of information processes and structures (modeling of various conditions and information system state environment during the experiment research), as well as soft calculations.

The scientific novelty of the research:

- *for the first time* there was developed a tuple model of basic risk characteristics which through the generalization of the basic characteristics, displayed by the six-component tuple, allows to create more flexible and effective methods for risks analysis and evaluation that take into account the possibility of forming the required amount of characteristics sets;
- *further development received* the methods of risks analysis and evaluation which, through the tuple model of the basic risk characteristics and the logical-linguistic approach at processing of dynamically changing sets of deterministic and fuzzy defined basic parameters, allow the creation of effective evaluation means with integrated capabilities;

- *for the first time* there were developed methods for implementing the function of *n*-fold incrementing of the number of terms with the use of a partial extension of the base, in which, by modifying by the *n*-fold extension of the function of terms incrementing by one order, extends the possibility of formalizing the process of equivalent transformation of the number of standard terms of a linguistic variable by n orders without involving the experts of the relevant subject area;

- *further development received* the methodology for the synthesis of IS risks analysis and evaluation systems, which allows to formalize the process of creating tools with flexible capabilities of specified sets use of processed values in the IS risks analysis and evaluation;

- *further development received* structural solutions of IS risks analysis and evaluation systems which, through subsystems for processing basic characteristics and generating data that implement the proposed methods, allow the formation and transformation of data both in qualitative and quantitative interpretation.

The practical significance of the research:

- on the basis of the proposed structural solutions of the systems and of the developed synthesis methodology there was constructed an algorithm for the implementation of the RAEM IS software;

- developed integrated databases of IR, threats and IS violation, which can be used at the construction of RAEM;

- on the basis of the proposed algorithm and integrated databases there was implemented the RAEM IS software, which uses and dynamically determines various sets of basic characteristics, that increases the flexibility, functionality and convenience of its use both in deterministic and in fuzzy, poorly formalized environment.

The results of the dissertation research were used in the educational process of the Information Security Department and Computer and Software Engineering Department of the KazNRTU named after K.I.Satpayev, of the Information Technology Security Department of the National Aviation University (Ukraine, Kiev), and in "DELTA" information systems security" Ltd. (Ukraine, Kiev) and in "QUARES" LLP (Almaty).

Approbation of the research results. The main points and results of the dissertation work were reported and discussed at various international conferences and seminars, including:

- seminars of the Computer and software engineering Department of the KazNRTU named after K.I.Satpayev;

- a scientific seminar "Modern Information Security Technologies" of the Information Security Department of the KazNRTU named after K.I.Satpayev;

- a scientific seminar of the Information Technologies Security Department of the National Aviation University (Ukraine, Kiev);

- International Satpayev Readings "The role and place of young scientists in the implementation of the program "Kazakhstan-2050", dedicated to the 80th anniversary of the KazNRTU named after K.I.Satpayev, Almaty, 2014;

- II International Scientific and Practical Conference "Information and Telecommunication Technologies: Education, Science, Practice" - Almaty, KazNRTU named after K.I.Satpayev, 2014;

- International Forum "Engineering Education and Science in the 21st Century: Problems and Prospects", dedicated to the 80th anniversary KazNRTU named after K.I.Satpayev, Almaty, 2014;

- III International Scientific and Practical Conference "Information Security of the "Kazakhstan-2050" Strategy, Astana, ENU named after L.N. Gumilev, 2015;

- XV International Scientific and Technical Conference "Problems of Informatics in Education, Management, Economics and Technology", Penza, 2015;

- Second International Scientific-Practical Conferenc "Problems of Infocommunications. Science and Technology ", Kharkiv, 2015;

- II International Scientific and Practical Conference "Topical issues of cybernetic security and information protection", Kiev, European University, 2016;

- International scientific and practical conference "Mathematical methods and information technologies of macroeconomic analysis and economic policy" (to the 80th anniversary of Academician A. Ashimov), Almaty, 2017.

The dissertation work was conducted within the framework of the scientific research project of KazNRTU named after K.I.Satpayev No. 757.MES.GF.15.IIT.6 "Research, harmonization, modification and registration of a standards group on the biometric support of information security" and of the scientific research work of the National Aviation University of Ukraine "Methodology of information systems security risks evaluation" (registration number 105 / 14.01.05).

Publications. There were published 20 scientific works, including 6 articles in the publications recommended by the Committee on control in the field of education and science of the Ministry of Education and Science of the Republic of Kazakhstan; 1 article was published in editions indexed in the Scopus database (Elsevier); 11 articles were published in the materials of international conferences; 2 articles were published in international journals.

Personal contribution of the applicant. The main points and results of dissertation work were received by the author independently. In the works, written in co-authorship, the personal contribution of the applicant is following: [20, 58, 59, 63] – there was carried out a risk concepts analysis and was developed a model of RTM; [77, 78] – were conducted the researches of risks analysis and evaluation tools using the proposed model; [79] – proposed two methods for IS risks analysis and evaluation of the First-RAEM and Second-RAEM; [80, 81] – proposed the method of *n*-fold incrementing of the number of terms of LV; [82, 83, 84] - developed a methodology for the synthesis of systems for IS risks analysis and evaluation and structural solutions of F First-RAEM and Second-RAEM systems; [85] - developed RAEM software on the basis of the presented methodology and

structural solutions, as well as carried out an experimental research of these systems. From the works, published in the co-authorship, there were used the results received by the applicant independently.

Structure and volume of the dissertation work. The dissertation work consists of an introduction, four sections, conclusion, a list of used sources from 83 points, appendices. The total volume is 147 pages and contains 43 figures and 57 tables.