Implementation of the model and algorithm for assessing the security of information in an automated system

E V Trapeznikov and L G Varepo

Omsk State Technical University, 11, Mira av., Omsk, 644050, Russia
E-mail: evtrapeznikov@yandex.ru

Abstract. New technologies provide much more progressive ways of working with information. Access to information is provided from anywhere, without geo-referencing. All this causes the emergence of new threats and vulnerabilities. An important task is to ensure the security of data, identify compliance of protection systems with the regulatory framework and current threats to information security. Timely audit allows to confirm the necessary level of security or to notify about its shortcomings. The paper presents a developed model for assessing the security of information using intellectual means. The software algorithm for auditing the security status of an automated system for an information security specialist has been implemented and tested. The article presents implemented software for auditing the system of protection of automated systems. The preliminary data of approbation of the developed algorithm and program complex are demonstrated.

1. Introduction

In the period of active implementation and use of information technologies in various spheres of human activity, there are various threats to the security and integrity of the data used. Information technologies provide the storage of data on electronic media and distributed networks, different information processing occurs by means of automated systems. Taking into account the development of the technologies it is needed to ensure information security.

During the life cycle of information from receiving, to storage and destruction it is necessary to conduct a quality audit of information security to prevent loss of information at any these periods. Quality audit determines compliance with regulatory and legal component and defines if the organization hardware-software complex of information security is up to date.

Currently, information is one of the main assets which has special value and must be properly protected [1]. In consequence, there is the problem of increasing number of threats and vulnerabilities.

1 Confidentiality guarantees access to information to only specified people.
2 Integrity ensures that only a certain number of people can change information.
3 Availability ensures the unhindered and constant access to information for only specified group of people.

When building information security systems, control processes of the adequacy of the measures and protection means, as well as identifying vulnerabilities in the existing information...
system, are important. Information security audit allows to carry out such monitoring and to identify new vulnerabilities [2,3,4,5].

Scientific school of Professor A. A. Shelupanov is actively involved in design of protection systems using various models of information security [6]. The authors are conducting research aimed at implementing and improving various types of information security mechanisms. The authors consider the issue of evaluating the security of information, in particular the developed model of documents workflow, which involves action on the information in completely different mediums [7].

Increased economic losses due to weak system of of the information protection and out-of-time the audit are considered in many papers [8, 9, 10]. The authors of [8] consider the impact of the relationship between internal audit and information security functions. The paper presents a research model that reflects the components of the audit system.

At the time of the audit the authors [11, 12] propose to integrate the process users to identify the specific human factors and possible risks. The authors propose to widely implement a system of active monitoring.

In [13], the authors present a model that includes many aspects of security, including attacks, detection, recovery, risk assessment and vulnerability reduction. Simulation of the system using the developed model allows to consider the dynamics of the system. Some studies are aimed at developing a model for assessing the necessity and effectiveness of the information systems audit [14, 15].

2. Statement of the problem
The analysis of the subject area studies identified the possibility of developing an assessment model of information security with intellectual means elements. This model is the basis for the algorithm and implementing software for an information security specialist, created in order to analyze and evaluate the quality of information security in the automated system. The relevance of the topic is justified by the development of technology and the widespread introduction of information technologies for information processing, storage and transmission.

3. Theory
The task of model development for auditing the security state of information is developing the algorithm, which allows to increase the quality and speed of audit. In addition, the algorithm should include the possibility of independent decision-making in certain cases. To solve the tasks, the following methods and techniques are used: theory of algorithms, database technology, expert evaluation method, the theory of artificial intelligence, methodology of protection of object-oriented programming.

The model assumes that the system must fully meet the requirements of the legislation in the field of information security system. Estimation of security is formed using criteria GOST R ISO/IEC 15408 Information technology (IT). Methods and means of security. Evaluation criteria for information technology security".

To develop assessment model of information security the block structure of the system is used in figure 1.

The collection of information starts in the "input data Analysis" block. Within this step, we define the composition of the test system (software, hardware, data bases, documentation, existing or proposed (or existing) network communication). The determination of the elements of the protection system, current settings, access levels, etc. are carried out on the survey basis. A list of questionnaires is generated for the survey. The results of the survey form part of the input for the unit is "Intelligent means".

The formation of the main requirements for information security system is based on the class of the used automated system, determined in accordance with the relevant documents.
To determine the class of an automated system is used the directive document of the Federal service for technical and export control "Automated systems. Protection against unauthorized access to information. Classification of automated systems and requirements on information protection".

The following parameters are used to define a class:

1. The level of information confidentiality.
2. The level of access to confidential information.
3. Mode of data processing.

Information that is generated for audit and security assessment is uploaded or downloaded from the Database block.

In addition, as the basis for the requirements formation for the information protection system, guideline documents FSTEC and the order of the FSTEC of Russia from February 11, 2013 N 17 "About the statement of requirements for protection of information not constituting a secret of state, contained in state information systems" are used.

All the necessary documentation, which is used throughout the schema model is formed from a Library block.

The obtained results of the preparatory phase provide generating a list of destabilizing factors on the basis of the data bank FSTEC (1), the local copy is stored in the Database block.

\[ S = \{S_1, ..., S_N\} \]  \hspace{1cm} (1)

where \( S \) is the set of destabilizing factors.

Block "Intellectual means" contains elements of the artificial neural networks theory. For this block, input parameters are the results of the survey and a number of destabilizing factors. All generated data help intellectual environment to perform the decision-making.
Figure 2. Algorithm for automated system software development.

In this block, the unit vectors are generated for input and output layer of a neural network. Every destabilizing factor has its own weight factor, which may vary in the process of the neural network training. The training is organized by the method "with a teacher". The neural network decides about the necessary measures depending on the possible destabilizing factors.

The resulting block of the entire model is "Results". At this stage the necessary documents about the shortcomings of the system and measures for its elimination are formed. References to the paragraphs of the legal documentation if are provided if necessary.

4. Software development

Software development is based on the algorithm, which is a step-by-step collection of information about the IT object for subsequent security assessment (audit) and the results generation in figure 2.

Software is developed using C# programming language (object oriented programming) and the development environment Microsoft Visual Studio 2017. The software incorporates a database as the main repository of all information circulating inside the development. As at the moment it is planned to use a local database without installing third-party software, for the realization, embedded cross-platform database SQLite was chosen, which supports a sufficiently complete set of SQL commands.

The software is based on the pattern of MVC development model, view, controller. Basic logic design and visual presentation are separated, thereby ensuring the scalability of development and easy transfer. To ensure the independence of the calculations and obtaining results from different blocks of the algorithm, the individual processes stand out in their own independent threads.

The software operation is based on the use of the access rights differentiation possibility. Assigned rights are determined depending on the fact which user is logged into the system. After login the user can start working. User passwords are stored in the database in encrypted form, thereby ensuring safety of the software operation. The first step is to create or open
Figure 3. Research result.

an existing project. The project is created for each system of protection. "Project" contains information about each iteration of the audit, the audit results, the results of intellectual means running, etc.

When creating a "project", it is made accessible only to the system administrator and the user who created it. The user may grant access to the current project to others with read-only rights.

The first step in the operation of the software is the class definition of the investigational automated system. For the definition of the class it is suggested to answer a series of questions drawn up in accordance with the governing document FSTEC. The security officer needs to properly assess the class for the appropriate images to produce an audit of the protection system and protection assessment information.

On the basis of the preparatory phase a survey is carried out and the results are generated. The obtained results are input to the intelligent block.

The next step is downloading into the software database or updating the list of current threats and vulnerabilities from the data bank of the FSTEC. From this list, many destabilizing factors are formed.

As a result of all the operations, the software creates documents, which contain all the results, not compliance with the requirements of legislation and guidance documents, and the list of possible threats that may be subject to an automated system in its current state.

5. Experimental results

The object of the research is the organization system of information security. For the analysis the data of 20 organizations were used, for each the different classes of automated systems were defined. For each organization a full cycle of studies were completed in figure 3. In accordance with it the following results compliance with systems for the protection of organizations were obtained.

The study shows that almost all organizations have high-quality security systems, with only a few exceptions. However, after the application of the intellectual means of calculation, possible threats have been identified. In the process of several runs, there was the neural network training
to reduce the errors of the first and second kind. That ultimately leads to increased accuracy of decision-making.

Due to the fact that the sample is small enough to reduce errors and increase the accuracy, it is required to increase the original values. With the current dataset, the errors of the first kind are 0.32.

6. Conclusion
The development of technologies and their widespread implementation requires special attention to the systems of information protection. The presented model and the implemented audit software for a information security specialist allows to solve a number of problems:

1. Boosting the audit conduction.
2. Improving the quality of the audit.
3. Using the list of relevant threats and vulnerabilities from the data bank FSTEC allows to maintain a system of auditing up-to-date.
4. The fact that elements of intellectual means allow to obtain possible solution when upgrading system protection.
5. The fact that saving the results of each audit at a particular organization provides tracking of changes in security system in dynamics.

References
[1] GOST R ISO/IEC 27002-2012 Information technology (IT). Methods and means of security. The regulation of information security management Standardinform 2014 p 210 (Russia)
[2] Makarenko S I 2018 Information security audit: main stages of the conceptual framework, activities classification Control, Communication and Security Systems 1 pp 1-29 (Russia)
[3] Dor D and Elović Y 2016 A model of the information security investment decision-making process Computers & Security 63 pp 1-13
[4] Trapeznikov E V 2017 Decision analysis for the evaluation of security of information in information systems Young Russia (Rossiya molodya): advanced technology into the industry! 2 pp 30-34 (Russia)
[5] Maksimenko V N and Vasyuk E V 2017 The main approaches to risk assessment and analysis of information security The Economy and the quality of communication systems 4 pp 42-48 (Russia)
[6] Shelupanov A A et al 2017 Current trends in the development of methods and means of information protection Proceedings of Tomsk state University of control systems and radioelectronics 20 pp 11-24 (Russia)
[7] Novohrestov A K 2017 et al 2017 The model of security threats to information and media Vestnik of Irkutsk state technical University 131 pp 93-104 DOI:10.21285/1814-3520-2017-12-93-104 (Russia)
[8] Steinbart P J et al 2018 The influence of a good relationship between the internal audit and information security functions on information security outcomes Accounting, Organizations and Society DOI: 10.1016/j.aos.2018.04.005
[9] Wei Y et al 2018 Performance evaluation of the recommendation mechanism of information security risk identification : Advances in Human-like Intelligence towards Next-Generation Web Neurocomputing 279 pp 48-53
[10] Piech H 2017 Audit expert system of communication security assessment: Knowledge-Based and Intelligent Information & Engineering Systems Procedia Computer Science 112 pp 147-156.
[11] Ki-Aries D and Faily S 2017 Persona-centred information security awareness Computers & Security 70 pp 663-674
[12] Boiko A and Shendryk V 2017 System Integration and Security of Information Systems Procedia Computer Science 104 pp 35-42
[13] Nazareth D L and Choi J 2015 A system dynamics model for information security management Information & Management 52 pp 123-134
[14] Herath H S B and Herath T C 2014 IT security auditing: A performance evaluation decision model Decision Support Systems 57 pp 54-63
[15] Steinbart P J, Raschke R L, Gal G and Dilla W N 2012 The relationship between internal audit and information security: An exploratory investigation International Journal of Accounting Information Systems 13 pp 228-243 DOI: 10.1016/j.accinf.2012.06.007