Filling a Knowledge Base for Expert System in Information Security

N Kireeva¹, I Pozdnyak¹, A Gazizulina²

¹Povolzhskiy State University of Telecommunications and Informatics, Information Security Department, Samara, Russia
²Peter the Great St.Petersburg Polytechnic University, St.Petersburg, Russia

Corresponding author’s e-mail: albinagazizulina@gmail.com

Abstract. This article describes a study of parameters of a comprehensive assessment of the organization’s information security. The formation of a knowledge base based on international and national standards and various industry requirements is proposed. Based on the standards, methods for filling the knowledge base for the expert system and a model for the functioning of this system are proposed. As a result, with a help of a specific user interaction algorithm with the output mechanism, it is possible to segregate the industry component in information security assessment process that will allow more accurate identification of risks and making recommendations for protection.

1. Introduction

Modern studies of information systems show that at present, any organization is engaged in storing or processing information, in addition, one way or another it deals with personal data, the protection of which is also assigned to the organization itself. The number of service are according by the Internet increased significantly. The analysis of the organizations using the Internet network in Russia in the per cent of the total number of the organizations shows that in 2005-2017 years the number of organizations using the Internet increased in 1.7 times. It is 88.9% (figure 1, figure 2). Proportion of the Internet users in Russia is 81% general public. Including 65% go online every day. At the same time, about 37%, according to data for 2017, use the Internet to purchase goods and services.

An important component in monitoring the international and national of information security in an organization is an audit, which consists in obtaining objective qualitative and quantitative assessments of the current state of security of an organization in accordance with certain criteria and safety indicators. As a rule, an audit requires the verifier to have in-depth knowledge of the legal framework in the field of protection, as well as the specifics of the data stored and processed in a particular information system owned by the organization [1-3, 7].

Existing audit systems are based on expert systems. Expert systems (ES), the most typical implementation of artificial intelligence, are now used in various areas for risk assessment. An important feature of expert systems is their ability to learn, which is associated with a continuous process of knowledge detection and data mining. That is why the first component of the expert system should be the knowledge base [4-6].

According to experts, in the near future, expert systems will play a leading role in all phases of design, development, production, distribution, sales, support and provision of services. Their technology, having received commercial distribution, will provide a revolutionary breakthrough in the integration of applications from ready intelligently interacting modules.
Among specialized knowledge-based systems, real-time expert systems, or dynamic expert systems, are most significant. They account for 70 percent of this market [8, 11-13].

One of the most important requirements for expert systems are:
- Ensuring the filling of the knowledge base of varying degrees of complexity with minimal time and labor.
- Providing problem and subject-oriented system configuration.
- Ensuring the creation and support of interfaces for various categories of users.
- Ensuring the level of information security (by user categories) and the prevention of unauthorized access.

Often while building the knowledge base for the expert system, the industry components remain unknown and unappreciated, which determines the relevance and practical significance of studying the problem stated in this article [14 – 16].
In connection with the dynamic development of information technologies and the widespread use of information systems of various architectures and difficulties in the activities of modern small enterprises, there is the problem of a comprehensive assessment system for information security. At the same time, a team of specialists is often needed to solve this problem.

The goal of the presented work is to create an Expert system, within which it is possible to conduct a comprehensive information security (IS) assessment for both a typical information system and an enterprise system for a particular industry (gas, energy, telecommunications, banking, etc.). It is planned to develop an algorithm for interaction between the user and the information system, which will allow, if necessary, to identify the sectoral component in the process of information security assessment, as well as to describe in detail the methodology for filling the expert system’s internal knowledge base.

2. Knowledge Base Analysis

As part of the process of comprehensive information security assessment of an information system, the creation of an expert system is possible, justified, relevant and under necessary condition. There are several reasons for this:
- the possibility of making a subjective decision inherent in a person is reduced to zero;
- it is possible to divide one large task into several subtasks;
- the use of a human expert is problematic and expensive (especially in small enterprises), and the use of ES allows you to reduce the number of specialists and experts to analyze and evaluate IS;
- the complexity of managing, analyzing and information security assessment leads to the fact that a person needs a lot of time in order to reach the level of an expert.

At the moment, expert systems are mostly focused very narrowly and do not always give the desired effect.

The scheme of functioning of the Expert systems in its general form is shown in figure 3.

![Figure 3. The interaction of elements of Expert systems](image-url)

The main elements of any ES is the Knowledge base (KB) and the logical inference unit. The Knowledge base must be sufficiently demonstrative and at the same time allow the construction of structural models of an information system, models of threats and vulnerabilities associated with individual components of the information system. This will allow to identify those elements and objects of the information system, the risk and damage from the violation of security of which is the most critical.
Today, when building an Expert systems knowledge base, the process of acquiring the necessary knowledge is the most laborious. In doing so, the knowledge engineer decides what method of knowledge engineering will be used, and how he will interact with the expert.

Conversations with an expert. In this group of methods distinguish observational and intuitive approaches.

With an observational approach, they follow the work of the expert, trying not to do anything that could affect the work of the expert in solving the problem. The observation is followed by the clarification stage, at which the knowledge engineer together with the expert analyzes the record of the expert’s stage of work, performed by the observer. This approach is also called protocol analysis.

In an intuitive approach, in one case, the expert acts as the developer of a model of his behavior when solving problems, in the second, as a knowledge engineer.

The expert choose is the principal question at the stage of formation of the knowledge base. The expert personality can be considered as a dynamic model. We will use the personality dynamic model described by Milovanov V.P. [9] like the expert, who will be a developer of the behavior model in solving problems, and as a knowledge engineer.

Let x is the expert x information (the expert x problems); y is the information for the expert from engineer. The expert gives the opinion (assessment) to the engineer y. We will have the next model:

\[
\begin{align*}
\frac{dx}{dt} &= \alpha_1 y + \alpha_2 xy - \alpha_3 x^2 y, \\
\frac{dy}{dt} &= \beta_1 x - \beta_2 xy. 
\end{align*}
\] (1)

Here \(\alpha_1, y\) is the engineer y knowledge, agreed with the expert x (\(\alpha_1\) - relevancy of expert x assessment), and \(\beta_1, x\) - is the expert x knowledge, agreed with the engineer y, 
\(-\beta_2, xy\) is the engineer y expectations, forwarded to the expert x, \(\alpha_2, xy\) is a part shows the expert x listens the engineer y and forms agreed answers on the proposals of the engineer y; 
\(-\alpha_3, x^2y\) shows the expert x listens the engineer y proposals, forms agreed answers on the proposals of the engineer y (multiplier \(x^2\)), forms the actions to bring in knowledge base.

The equilibrium position of the model (1) is:

\[
\begin{align*}
x &= \frac{\alpha_2 \pm \sqrt{\alpha_2^2 + 4\alpha_3\alpha_1}}{2\alpha_3}, \\
y &= \frac{\beta_1}{\beta_2}.
\end{align*}
\] (2)

The values of \(\sigma\) and \(\Delta\) are as follows:

\[
\begin{align*}
\sigma &= \alpha_2 y - 2\alpha_3 xy - \beta_2 x, \\
\Delta &= \beta_2 xy(2\alpha_3 x - \alpha_2).
\end{align*}
\] (3)

When \(2\alpha_3 x > \alpha_2\) and \(2\alpha_3 xy + \beta_2 x\) there is a bifurcation and an expert arises, whose opinions are reliable.

We now calculate the Lyapunov dimension \(\alpha\):
\[
\alpha = \frac{\pi}{4 \left( a_1 + a_2 x - a_3 x^2 \right)} \left\{ \left( a_2 y - 2a_3 x y \right) \left( \beta_1 - \beta_2 y \right) \left( a_2 - 2a_3 x \right) + \left( a_2 y - 2a_3 x y \right) \right\} \\
\left( a_1 + a_2 x - a_3 x^2 \right) \left( \beta_1^2 + a_1 \beta_2 y \right) - 2 \left( a_2 y - 2a_3 x y \right) \left( a_1 + a_2 x - a_3 x^2 \right) \left( \beta_1 \beta_2 y \right) \left( a_2 y - 2a_3 x y \right) \left( \beta_1 - \beta_2 y \right) \left( a_2 - 2a_3 x \right) \] \\
+ a_3 y \left( a_2 - 2a_3 x \right) \left( a_1 + a_2 x - a_3 x^2 \right) \left( \beta_1 - \beta_2 y \right) \left( a_2 y - 2a_3 x y \right) \left( \beta_1 \beta_2 y \right) \left( a_2 - 2a_3 x \right) \] \\
- \left( a_2 y - 2a_3 x y \right) + \left( a_1 + a_2 x - a_3 x^2 \right) \left( \beta_1 - \beta_2 y \right) \left( a_2 y + 2a_3 x y \right) \alpha_3 \]

(4)

Because, obviously, the value \( \alpha \) can be both positive and negative, it means that expert \( x \) gives consistent or inconsistent estimates.

The position of the equilibrium of the value of the opinion (assessment) of the expert and the engineer will fall into the knowledge base \( (C_1, C_2 = 1) \).

3. Assessment Filling Knowledge Base

In our work, we will build a knowledge base on the basis of international and national standards in the field of information security and various industry documents (International and national standards, Industry standards, Working documentation, Technical requirements, Industry recommendations). In addition to this, a knowledge engineer will prepare a series of typical tasks for discussion with an expert.

To begin, consider the standard ISO/IEC 27002 “Information technology – Security techniques – Code of practice for information security management”. Section 6.1 “Internal organization” consider information security management issues in an organization. To create the Knowledge base, we use subsections 6.1.1 - 6.1.8. Each contains questions necessary for consideration. For example, does the organization have an information security council (clause 6.1.2), are information security responsibilities distributed (clause 6.1.3), is there an independent audit (audit) of information security (clause 6.1.8) and etc. Questions of section 6.2 “External Parties” (touches issues of supporting security of organization’s information processing tools and information assets when accessed by third parties) will be included in the knowledge base. Application of Section 7 “Asset Management” in the knowledge base helps to determine the assets in relation to which the information security assessment will be carried out, as well as the appropriate protection of the organization’s selected assets. Should not be overlooked and organizational measures relating to the actions of staff. To do this, apply Section 8 “Human Resources Security”. This includes taking security issues into official duties when hiring personnel (clause 8.1.1), and user training (clause 8.2.2), and issues related to the transformation or change of employment of employees (clause 8.3). Section 9 “Physical and Environmental Security” contains the necessary information for the developed knowledge base on protected areas, equipment safety inside these areas, as well as general measures to control IS. Section 10 “Communications and Operations Management” will help fill the knowledge base with information about:

- operational procedures and responsibilities,
- management of third party services,
- planning and acceptance of systems,
- protection against malicious and mobile programs,
- reservations
- network security management,
- handling media,
- exchange of information,
• e-commerce service,
• monitoring.

Section 11 "Access Control" will allow filling the knowledge base of the ES with knowledge of:
• access control business requirements
• user access management,
• user responsibilities
• network access control,
• control of access to the operated system,
• control access to information and application programs
• mobile computing and remote work.

Issues related to Section 12 "Information Systems Acquisition, Development and Maintenance", Section 13 "Information Security Incident Management", Section 14 "Business Continuity Management" and Section 15 "Compliance", will also be fully included when creating the knowledge base. More fully with these sections can be found in ISO/IEC 27002.

Next, we consider the standard ISO/IEC 27001 “Information technology. Security techniques. Information security management systems. Requirements”. Appendix A of this standard contains the objectives and management measures that are closely related to ISO/IEC 27002. Therefore, when filling the knowledge base of the developed expert system, care should be taken to prevent the repetition of similar situations. For example, section A.5 of the appendix corresponds to section 5 “Security policy” (ISO/IEC 27002), section A.12 of the appendix - with section 12 “Acquisition, development and maintenance of information systems” (ISO/IEC 27002). An exception is Section A.13, Information Security Incident Management. Section 13.2 “Information Security Incident Management and Necessary Improvement” (ISO/IEC 27002) partially complies with it.

Despite this, the objectives and management measures from Appendix A (ISO/IEC 27001) are mandatory for inclusion in the knowledge base. If they do not override the measures and methods of managing information security systems (ISO/IEC 27002), then they are their complement. The list of management measures contained in these two standards is not exhaustive and can be supplemented by a knowledge engineer and expert.

The following standard to which attention should be paid when filling the ES knowledge base is ISO/IEC 27005 « Information technology - Security techniques - Information security risk management». The knowledge base should include the types of assets for which risks will be assessed:
• Business processes (or subprocesses) and business activities;
• Information;
• Hardware;
• Data processing equipment (active);
• Mobile equipment;
• Stationary equipment;
• Peripheral processing equipment.
• Data carrier (passive)
• Electronic media.
• Software
• Operating system.
• Software maintenance, maintenance or administration.
• Batch software or standard software.
• Business application, etc.
• Standard business application.
• Specific business application.
• Network
• Wednesday and support.
Passive or active repeaters.
Communication interface, etc.

Also in the knowledge base must make the concept of "asset value". At the same time, it should be determined by the owners and users of assets in the process of using the expert system. In addition, the concepts of "threat", "source of threat", "object of threat", "probability of threat realization", "vulnerability", "degree of vulnerability", and "protective measures" should be introduced. A list of typical types of threats is presented in Appendix C of the standard, examples of common vulnerabilities are given in Appendix D of ISO/IEC 27005.

In total, four national standards in the field of information security formed the basis of the knowledge base of the developed expert system. They contain the most important information (knowledge), reflecting a comprehensive information security assessment of the information system of any enterprise. In addition, it is necessary to consider and include in the KB data of various industry documents. Since there are a huge number of industries, it is not possible to include all possible standards and recommendations. However, the knowledge base should be filled with documents from the most sought-after industries. For example, the banking sector. For him, there are a number of standards that will help fill the BS with industry knowledge: STO BR IBBS-1.0-2008, STO BR IBBS-1.1-2007, STO BR IBBS-1.2-2009, RS BR IB IBBS-2.0-2007, RC BR IB IBS-2.2-2009.

One of the main standards is the Bank of Russia standard: “Ensuring the information security of organizations of the banking system of the Russian Federation. General provisions “(STO BR IBBS-1.0-2008). Section 7 of this document will allow defining information security requirements for assigning and distribution roles and ensuring confidence in personnel, information security requirements for automated banking systems at life cycle stages, as well as requirements for ensuring information security in access control and registration, in the use of Internet resources, in the use of cryptographic information protection, banking payment and information technology processes. Section 8 “Information Security Management System of Organizations of the Banking System of the Russian Federation” examines in detail the information security management, which will fully fill the knowledge base with information on the banking industry.

During the filling of the Knowledge Base with the help of industry standards it is necessary to remember that situations, questions and knowledge can already be entered into the database. In this case, you should check the nuances associated with a particular industry.

4. Conclusion
The proposed algorithm for filling the knowledge base, as well as building an expert system, allows for a comprehensive assessment of the information security of an enterprise taking into account the industry component, which is a necessary and important condition during an information security audit. The interaction of the Expert system user with the output mechanism will be carried out using a specific algorithm that, if necessary, will allow to highlight the component for the industry in the information security assessment process. The result of this interaction will be the recommendations issued by the system on the protection of the selected asset, and the main risks will be identified. Based on the results of the expert audit, preparation of administrative documents is being carried out, which determine recommendations for building or upgrading the existing information protection system. In addition, this algorithm for filling the expert system knowledge base will reduce the financial and time costs for conducting an audit.

Acknowledgment
The research carried out with the financial support of the grant from the Program Competitiveness Enhancement of Peter the Great St. Petersburg Polytechnic University.
The section «Knowledge Base Analysis» is based on the financial support of the Council on Grants of the President of the Russian Federation (Project No. MK-3229.2018.8 "Improving the Standardization Management Method"). Peter the Great St. Petersburg Polytechnic University.

References

[1]. Bataev, A. V. (2017). Analysis of the use of cloud services and assessment the possibilities of introducing in Russian financial institutions. Paper presented at the Proceedings of the 29th International Business Information Management Association Conference - From Regional Development Sustainability to Global Economic Growth, 25-35.

[2]. Demidenko, D. S., Malinin, A. M., & Litvinenko, A. N. (2017). A new classification of the risks of the quality processes. Paper presented at the Proceedings of the 30th International Business Information Management Association Conference, IBIMA 2017 - Vision 2020: Sustainable Economic Development, Innovation Management, and Global Growth, 2017-January 2892-2897.

[3]. Didenko, N. I., Skripnuk, D. F., & Mirolyubova, O. V. (2017). Big data and the global economy. Paper presented at the Proceedings of 2017 10th International Conference Management of Large-Scale System Development, MLSD 2017, doi:10.1109/MLSD.2017.8109611

[4]. Klochkova, E. S., Bolsunovskaya, M. V., & Shirokova, S. V. (2019). The significance of humanities for engineering education. Paper presented at the Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, PTES 2018, 265-268. doi:10.1109/PTES.2018.8604199

[5]. Didenko, N. I., Skripnuk, D. F., Kikkas, K. N., Sevashkin, V., Romashkin, G., & Kulik, S. V. (2018). Innovative and technological potential of the region and its impact on the social sector development. Paper presented at the International Conference on Information Networking, 2018-January 611-615. doi:10.1109/IICOIN.2018.8343191

[6]. Didenko, N., Skripnuk, D., Mirolyubova, O., & Radion, M. (2017). Analysis of rural areas development of the region using the ADL-model. Paper presented at the Research for Rural Development, 2 142-147. doi:10.22616/rd.23.2017.061

[7]. Glukhov, V. V., Ilin, I. V., & Iliahenko, O. J. (2016). Improving the efficiency of architectural solutions based on cloud services integration doi:10.1007/978-3-319-46301-8_43

[8]. Gorodetskiy, A. E., & Tarasova, I. L. (2019). Situational control a group of robots based on SEMS doi:10.1007/978-3-319-99759-9_2

[9]. Milovanov V.P. (2005) Sinergetika i samoorganizatsiya. Obshchaya i sotsial'naya psikhologiya /USSR, p.208

[10]. Ilin, I. V., Iliashenko, O. Y., & Levina, A. I. (2016). Application of service-oriented approach to business process reengineering. Paper presented at the Proceedings of the 28th International Business Information Management Association Conference, 768-781.

[11]. Klochkov, Y., Klochkova, E., Antipova, O., Kiyatkina, E., Vasilieva, I., & Knyazkina, E. (2016). Model of database design in the conditions of limited resources. Paper presented at the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016: Trends and Future Directions, 64-66. doi:10.1109/ICRITO.2016.7784927 Retrieved from www.scopus.com

[12]. Kostin, G. A., Pokrovskaya, N. N., & Ababkova, M. U. (2017). Master-chain as an intellectual governing system for producing and transfer of knowledge. Paper presented at the Proceedings of 2017 IEEE 2nd International Conference on Control in Technical Systems, CTS 2017, 71-74. doi:10.1109/CTSYS.2017.8109491

[13]. Kovalenko, I. I., Sokolitsyn, A. S., & Sokolitsyna, N. A. (2018). The enterprise's automated management stability system taking into account its life cycle stage. Paper presented at the Proceedings of the 2018 5th International Conference "Quality Management, Transport and Information Security, Information Technologies", IT and QM and IS 2018, 357-360. doi:10.1109/ITMQIS.2018.8524966

[14]. Kozlovsky, V., Klochkov, Y., Ostapenko, M., Ushanova, N., & Antipov, D. (2016). Conformity assessment of car quality databases exemplified on the case of the russian car manufacturer 'auto VAZ'. Paper presented at the 2016 5th International Conference on Reliability, Infocom Technologies and Optimization, ICRITO 2016: Trends and Future Directions, 57-60. doi:10.1109/ICRITO.2016.7784925
[15]. Naidenova, X., Parkhomenko, V., & Curbatov, S. (2017). A neural-network like logical-combinatorial structure of data and constructing concept lattices. Paper presented at the CEUR Workshop Proceedings, 1921 62-76.

[16]. Pechenkin, A., & Demidov, R. (2018). Applying deep learning and vector representation for software vulnerabilities detection. Paper presented at the ACM International Conference Proceeding Series, doi:10.1145/3264437.3264489