Method of development of information security expert system

Tynarbay Marzhan
L.N.Gumilyov Eurasian National University
Astana, Kazakhstan
tinarbai@bk.ru

***Abstract*—In the modern world, information technology is used in almost all spheres of society, so information security is particularly relevant. There are various methods of solving information security problems, one of which is the use of expert systems. This article discusses the method of development of information security expert system on Exsys Corvid.**

***Keywords*—information security, expert system**

Credit card information leaks, identity theft, ransomware, intellectual property theft, privacy breaches, denial of service-these information security incidents have become common news. Among the victims are the largest, wealthiest and most secure enterprises: government agencies, large retail chains, financial institutions, even manufacturers of information security solutions. Among the threats to the organization can be identified:

- Theft of confidential information, site deface, phishing, ransomware.
- Data loss due to natural phenomena or accidents.

Security is closely connected with IT infrastructure management: a well-managed network is more difficult to hack than a poorly managed one. To understand how well an organization protects information, the following questions arise, such as do you know what do your employees connect to their computers? What devices are connected within the local network? Do you know what software is used in your information systems? Did you configure your computers to meet information security requirements? Do you control employees ' access to confidential information or those who have elevated access rights in the systems? Do your employees understand their role in protecting your organization from information security threats? There are various methods of solving IS problems, one of which is the use of expert systems (ES). The possibility of using expert systems to solve problems of information security has become of interest to specialists in information security due to the the rapid development of information technology, hence the emergence of new types of threats. Already expert systems are used to solve some problems of information security:

- risk assessment and threat modelling;
- antivirus software;
- audit of information security of the enterprise.

Business disruptions in the form of data breaches, hacking, hijacking of website or social network accounts and IT infrastructure threats are part of the new business reality for organizations in any sector. The use of ES contributes significantly to the detailed analysis and evaluation of IS and the protection of the organization and its information assets from current and future cyber threats by specific information security specialists in various organizations without the involvement of additional and more qualified personnel. The main purpose of ES is that they act as a kind of assistant or amplifier of intellectual activity of a specialist in a particular subject area.

The generalized structure of the expert system is shown in Fig. 1. It should be noted that real ES can have a more complex structure, but the blocks shown in the figure are certainly present in any real expert system, since they represent the standard of the modern structure of the ES.

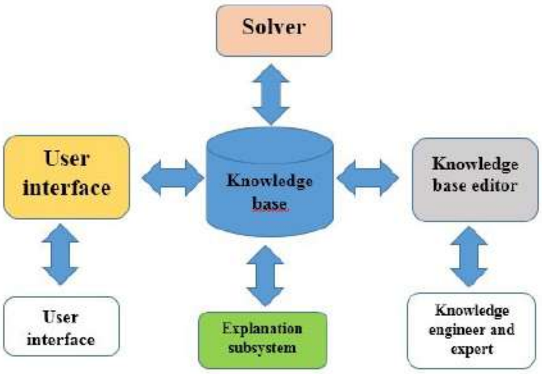


Figure 1. Structure of the expert system

Main components of IT used in the expert system: User interface, knowledge base (KB), knowledge engineer (ornithologist, interpreter engineer, analyst), expert, solver General scheme of interaction between the creators of the expert system is shown in Fig. 2.

In the course of work on the creation of ES, a certain technology of their elaboration has developed, including the following six stages: identification, conceptualization, formalization, implementation, testing, trial

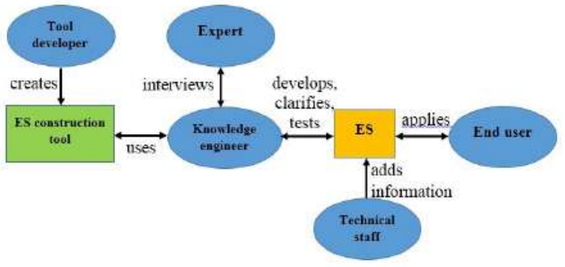


Figure 2. Interaction of the creators of the expert system

operation (Fig. 3). At the identification stage, the tasks to be solved are determined, the development goals are identified, experts and types of users are determined. At the stage of conceptualization, a meaningful analysis of the problem area is carried out, used concepts and their interrelations are revealed, the methods of problem solving are determined.

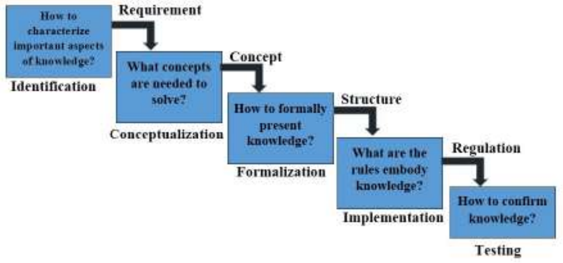

How to characterize important aspects of knowledge?
Requirement
Identification
What concepts are needed to solve?
Concept
Conceptualization
How to formally present knowledge?
Structure
Formalization
What are the rules embody knowledge?
Regulation
Implementation
How to confirm knowledge?
Testing

Figure 3. The stages of development of expert systems

At the stage of formalization, the methods of representation of all types of knowledge are selected and determined, the basic concepts are formalized, the ways of interpretation of knowledge are determined, the work of the system is modeled, the adequacy of the goals of the system of fixed concepts, methods of decisions, means of representation and manipulation of knowledge is assessed.

At the stage of implementation, the expert fills the knowledge base. Due to the fact that the basis of ES is knowledge, this stage is the most important and the most time-consuming stage of ES development. The process of acquiring knowledge is divided into the extraction of knowledge from the expert, the organization of knowledge that ensures the effective operation of the system, and the presentation of knowledge in the form of a understandable ES. The process of acquiring knowledge is carried out by a knowledge engineer based on the analysis of the expert's activities to solve real problems. The method of development of expert systems is shown in Fig. 4.

However, already at the initial stages, serious fundamental difficulties have emerged that prevent the wider spread of ES and seriously slow down and complicate their development. They are quite natural and follow from the very principles of the development of ES (tab. I).

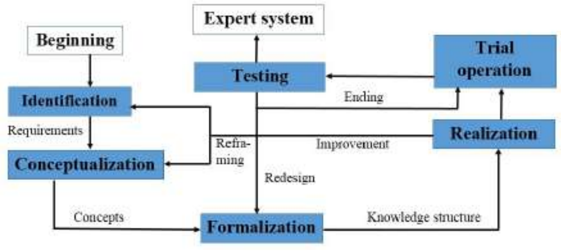


Figure 4. Methods of development of expert systems

Table I
PROBLEMS ENCOUNTERED IN THE DEVELOPMENT OF ES

Expert	Error in expert knowledge such as incorrect and incomplete knowledge
Knowledge engineer	Semantic errors due to different interpretations of the meaning of the knowledge engineer and the expert; Incomplete knowledge of the expert.
Knowledge base	Syntax errors in the forms of knowledge representation; Errors in content due to incorrect and incomplete knowledge, as well as uncertainty in rules and facts
Logical output machine	Errors in the logical output machine and in other software tools of expert systems
The output target	Inference errors due to incorrect prioritization of rules, interaction of rules and errors in the knowledge base; Error due to non-monotonic inference.

A lot of tools are presented on the market for the development of ES. One of the leaders is a system EXSYS CORVID.

Consider the example regarding the protection of information of any organization. Hereinafter there will be a description on how to use the Corvid Exsys shell to create an ES.

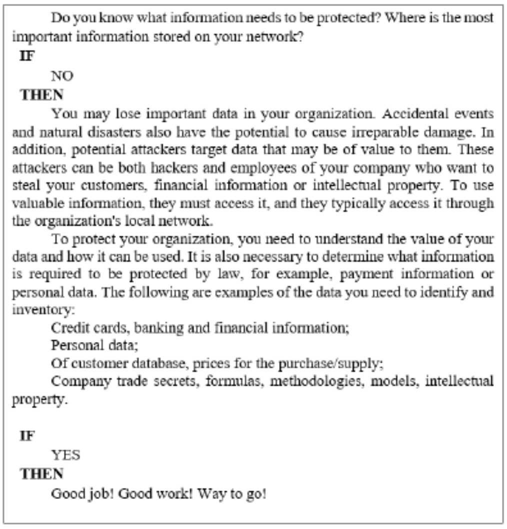
In the beginning, in order to move forward on the issue of information security, it was necessary to deal with the local network, connected devices, critical data and software. Without a clear understanding of what you need to protect, it will be difficult for you to ensure that you are providing an acceptable level of information securi.

Key issues that are necessary for our system:

Do you know what information needs to be protected? Where is the most important information stored on your network? Do you know which devices are connected to your network? Do you know what software is installed on employees ’ computers? Do your system administrators and users use strong passwords? Do you know which online resources are used by your employees (i.e., working or sitting in social networks)? Consider the question: do you Know what information you need to protect? Where is the most important information stored on your network?

To solve this problem, the variable "Know your infrastructure"was set.

In the simplest case, you can write only 2 rules:



Do you know what information needs to be protected? Where is the most important information stored on your network?

IF

NO

THEN

You may lose important data in your organization. Accidental events and natural disasters also have the potential to cause irreparable damage. In addition, potential attackers target data that may be of value to them. These attackers can be both hackers and employees of your company who want to steal your customers, financial information or intellectual property. To use valuable information, they must access it, and they typically access it through the organization's local network.

To protect your organization, you need to understand the value of your data and how it can be used. It is also necessary to determine what information is required to be protected by law, for example, payment information or personal data. The following are examples of the data you need to identify and inventory:

Credit cards, banking and financial information;

Personal data;

Of customer database, prices for the purchase/supply;

Company trade secrets, formulas, methodologies, models, intellectual property.

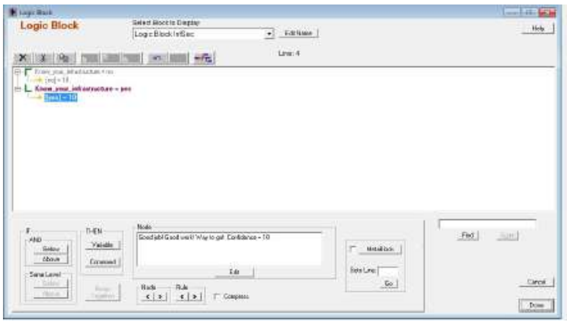
IF

YES

THEN

Good job! Good work! Way to go!

When all necessary variables are defined, logical blocks are built (Fig. 5), which describe the knowledge in the system. A logical block can contain one or more logical trees and/or rules.

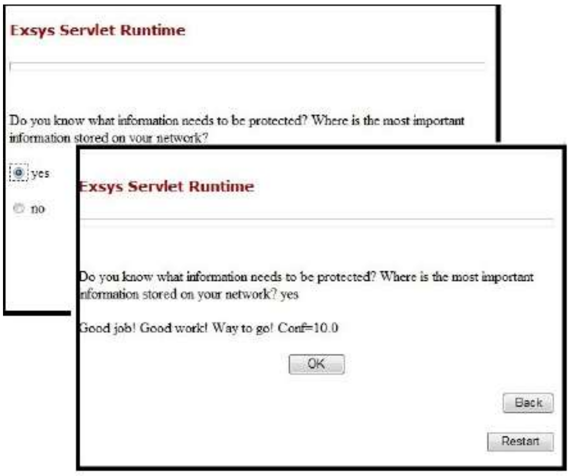


Good job! Good work! Way to go! Confidence = 10

Figure 5. Window logic blocks in the system Exsys Corvid

The user dialog after starting the ES will look as shown in Fig. 6 and Fig. 7.

The result is a very flexible and powerful development environment that can be quickly explored and implemented.Thus, a prototype was developed using Exsys Corvid, but the prototype should be improved with the help of new knowledge.



Do you know what information needs to be protected? Where is the most important information stored on your network?

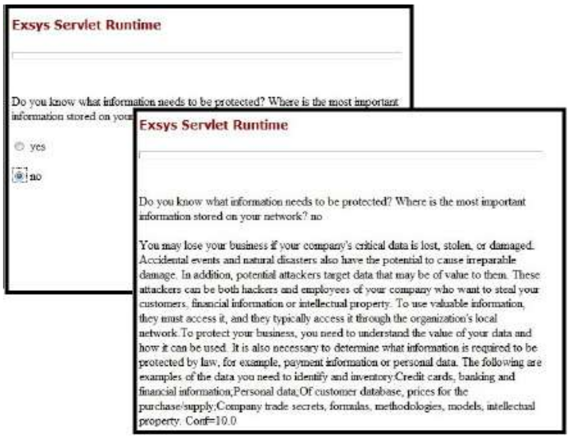
● yes

○ no

Do you know what information needs to be protected? Where is the most important information stored on your network? yes

Good job! Good work! Way to go! Conf=10.0

Figure 6. Window logic blocks in the system Exsys Corvid



Do you know what information needs to be protected? Where is the most important information stored on your

○ yes

● no

Do you know what information needs to be protected? Where is the most important information stored on your network? no

You may lose your business if your company's critical data is lost, stolen, or damaged. Accidental events and natural disasters also have the potential to cause irreparable damage. In addition, potential attackers target data that may be of value to them. These attackers can be both hackers and employees of your company who want to steal your customers, financial information or intellectual property. To use valuable information, they must access it, and they typically access it through the organization's local network.To protect your business, you need to understand the value of your data and how it can be used. It is also necessary to determine what information is required to be protected by law, for example, payment information or personal data. The following are examples of the data you need to identify and inventory.Credit cards, banking and financial information;Personal data;Of customer database, prices for the purchase/supply;Company trade secrets, formulas, methodologies, models, intellectual property. Conf=10.0

Figure 7. Window logic blocks in the system Exsys Corvid

The expert system can be used to analyze and configure information security systems. This conclusion is made on the basis of its main characteristics, properties, analyses, methods of development. However, for use in real-world tasks requires a fairly large data and knowledge base. Further work will be directed towards finding the sources of this data and knowledge. Also, it is possible to carry out additional studies to further define the task, by a more detailed description of the input data. If you develop an expert system that will have the following features:

- automation of risk assessment procedures;
- the assessment should be based on the established list of parameters;
- low requirements to qualification of the expert;
- presentation of the final assessment in a visual form;
- ability to easily adapt to the requirements of new or updated regulatory documents on is;
- formation of a list of recommendations to improve the organization's is system based on the results of the program.

With the above features, the expert system will most effectively assess the risks of violation of is organizations.

References

[1] Sapozhnikov A. Yu., Krivosheev I. A. Application of expert systems in the design process of aviation gas turbine engines // Molodoi uchenyi. 2009. 12. pp. 90-97. URL https://moluch.ru/archive/12/972/.

[2] D.I. Muromtsev. Exsys Corvid expert system shell. SPb: SPb GU ITMO, p.69, 2006.

[3] Kirilov P., Information security guidelines for small and medium-sized businesses (SMB) - URL https://habr.com/post/348892/

[4] Giarratano George., Riley G. Expert systems. Principles of development and programming. M.: Izdat. house ”Williams”, 2007. 1152 p.

[5] E. N. Sozinova Application of expert systems for analysis and evaluation of information security. Young scientist, 2011, 10, Vol.1. Pp. 64-66. URL https://moluch.ru/archive/33/3766/ (accessed: 10.01.2019)

МЕТОД РАЗРАБОТКИ ЭКСПЕРТНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Маржан Тынарбай

В современном мире информационные технологии используются практически во всех сферах жизни общества, поэтому информационная безопасность очень актуальна. Существуют различные методы решения проблем информационной безопасности, одним из которых является использование экспертных систем. В данной статье рассматривается методика разработки экспертной системы информационной безопасности на Exsys Corvid.

Received 10.01.19