Some Issues of Development of Intelligent System for Information Security Auditing

Kanat T. Kozhakhmet, Gerda K. Bortsova, Lyazzat B. Atymtayeva

***Abstract*— To ensure a good level of security any organization should conduct regular audits of information security. This process is highly expensive in terms of time, cost, and human resources. Automating the audit process through the development of the software can be a good alternative that will reduce costs, speed up the process of audit and improve quality by compliance it with international security standards. We also believe that automation of the audit process should be made by development of fuzzy expert systems, which provide the significant advantages by using in audit area. This paper suggests a way to develop Fuzzy Expert Systems in Information Security Auditing.**

***Index Terms*—expert systems, fuzzy logic, security audit**

I. INTRODUCTION

In connection with the development of information technology the organizations are increasingly faced with a wide range of potential threats to information security (IS), and as a consequence, more and more interested in ensuring a high level of its protection.

One of the best ways to assess, provide and maintain information security is to conduct its regular audit. Security Audit (in the broadest sense) is a complex, multistage and time-consuming process involving highly qualified specialists (experts), that makes it a pretty expensive service. There are a large variety of audit types including certain security standards (e.g., ISO 2700X) compliance audits.

Typically, an audit of information security consists of the following steps [1]:

1. Scoping and pre-audit survey: determining the main area of focus; establishing audit objectives.
2. Planning and preparation: usually involves the generation of an audit work plan.
3. Fieldwork: gathering evidence by interviewing staff and managers, reviewing documents, printouts and data, observing processes in action, etc.
4. Analysis: desperately sorting out, reviewing and trying to make sense of all that evidence gathered earlier.
5. Reporting: figuring out how to relate what was actually examined and found back to the original audit objectives, then gradually writing it all up.
6. Closure.

Each stage is accompanied by a large amount of information to be collected, sorted and analyzed. One of the measures taken to reduce costs and facilitate the audit process is the use of special tools such as checklists and questionnaires, to identify gaps between certain security standards and existing organization's security practices.

For example, a questionnaire with ISO 17799 Checklist ([2]) provides a number of audit questions (such as, for example, " Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.") Each of the questions corresponds to a specific section of the standard (e.g., 4.1.3 in the previous example). ISO IEC 27002 2005 (17799) Information Security Audit Tool, described in [3], offers several hundreds of audit questions, stated in the "yes-no" answers form (e.g., question like "Have you reduced the risk of theft, fraud, or misuse of facilities by making sure that all prospective employees understand their responsibilities before you hire them?"). The standard recommends to indicate the best security practices that need to be implemented and the actions to be taken, if the answer to the question is "no".

Thus, the auditing may be viewed as a process of asking questions, analyzing answers and producing recommendations.

All of the above tools are very useful for auditors and security personnel. Unfortunately the questionnaires don't give an overall impression of the whole security level in the organization. They are too general, not related to the actual policies of organization, its procedures, and etc. Therefore it is necessary to consider a special range of issues with the using of additional security measurements.

Another effective tool for the audit is to develop a knowledge base that will provide information for Chief Information Security Officers (CISOs) and will help them to find the right management decisions on the information security policy [4].

Key components of the knowledge base are: "Asset", "Source" (standard), "Vulnerability," "Step" (a refinement of the part of "Guideline" in a special section of the standard) and others.

Every "Step" refers to the protected Object, to the type of Vulnerability it is against as well as to the cross-references to other stored Guidelines. This tool provides search-based knowledge management directives, standards, analysis of

This work is a part of Research Project that is supported by Ministry of Education and Science in Republic of Kazakhstan on 2012-2014 years

Kanat T. Kozhakhmet with the Kazakh-British Technical University, Almaty, Republic of Kazakhstan (phone: 8-727-272-15-02; fax: 8-727-250- 46-51, e-mail: kanik85@gmail.com

Gerda K.Bortsova with the Kazakh-British Technical University, Almaty, Republic of Kazakhstan (phone: 8-727-272-15-02; fax: 8-727-250- 46-51, e-mail: gerdabortsova@gmail.com

Lyazzat B. Atymtayeva with the Kazakh-British Technical University, Almaty, Republic of Kazakhstan (phone: 8-727-272-15-02; fax: 8-727-250- 46-51, e-mail: atymtayeva@gmail.com, l.atymtayeva@kbtu.kz)

the components and issuing recommendations. As a result, the so-called meta-model of the security standard recommendations could be constructed.

By the reason of highly expensive process of information security Auditing in terms of high cost of different resources (time, people, expenses) the reducing the cost of the audit process is a priority for any organization. Automating the audit process by creating intelligent software (expert system) can significantly reduce costs, since the main work on decision-making is carried out automatically, based on computer analysis of the situation and issuing guidelines and recommendations.

II. Fundamentals of Expert System in IS Audit

As it's known, the expert system (ES) is a computer system that emulates the decision-making ability of a human expert. (Jackson 1998). The knowledge in expert systems, commonly represented in form of IF-THEN type-rules, may be either expertise or knowledge that is generally available from written sources [5].

We suppose that in the system of IS auditing, along with human knowledge, recommendations of security standards (such as ISO/IEC, COBIT and ITIL) can also serve as a source of expertise and may be translated into rules.

We consider implementing question-answer interaction between user and system, similar to checklist and questionnaire principle: ES will take user's answers on auditing questions, analyze them, and output a result in form of recommendations.

A little more detailed procedure of audit, performed by the expert system may consist from the following steps:

1. Company information acquisition: defining assets to be protected (equipment, data, etc.). Depending on this, the system will prepare some general questions to start from.
2. Process of obtaining information by the system from personnel by asking appropriate (possible in particular situation of the organization, described in stage 1) questions.
3. Expert system's logical inference.
4. The system produces the output as a list of recommendations.

In comparison with the audit process described in the previous section this procedure looks much easier. So we can automate some stages of the audit.

In addition, the development of expert systems in the field of information security has many advantages. Let us consider some of the advantages of using expert systems (in accordance with [5]):

• Reduced cost. Development of an expert system is relatively inexpensive. Taking into consideration an opportunity of repeated use by multiple organizations, the cost of the service per client is greatly lowered.

• Increased availability. Expert knowledge becomes available using any suitable device at any time of the day. Web-based expert systems open up ability to access expertise from any Internet connected device. In some sense, "expert system becomes the mass production of expertise." (Giarratano & Riley 1998)

• Multiple expertises. Using knowledge from multiple sources increases total level of expertise of the system. In case of Information Security, a combination of number of recommendations of security standards and knowledge of several independent specialists could improve the expert estimation.

• Time saving. IS auditing is a time consuming process. Expert systems at some phases of audit (analysis of gathered evidence, reporting) can save days (or weeks) by faster responding (in comparison with a human expert) and reducing amount of paper work.

• Steady, unemotional, and complete response at all times. By the use of programs, human factor influence decreases.

We believe that developing web-based Expert System in Information Security Audit (ESISA), from the first, practical point of view, will save time and money of companies-clients, and, from the second, scientific idea, it will be a good fundamental experience for further development of methodologies for applying Artificial Intelligence techniques in the area of Information Security.

Previously expert systems approach in security area was applied in computer security auditing. An Expert System in Security Audit (AudES), designed for automating some audit procedures, like identifying potential security violations by scrutinizing system logs, is described in [6].

But the application of the methodology of expert systems in IS auditing in the broadest sense (not only in computer security) (what actually we would like to realize) remains largely untouched. Our task is to study and solve the problems of development of expert systems in a wide range of information security audit, which includes aspects of computer security.

Information security is usually divided into administrative, physical and computer security. We plan to use each of these types in our system. Based on the family of ISO 2700X standards, it is possible to highlight some aspects of security such as: asset management (corresponding chapter 7 of the ISO), human resource security (compliance with chapter 8 of ISO), communication and operation management (chapter 10), access control (chapter 11), incident management (chapter 13), and etc. By using the approaches for managing uncertainties through the application of fuzzy set and logic theory, we can extend and improve the development of ESISA system. The reason is opinion that the remarkable human ability to make rational decisions in an environment of imprecision is based on his using the tolerance for uncertainty [7].

III. Processing of Uncertainties

We suppose that the task of developing expert system for IS audit on a large scale requires the use of methods more sophisticated than the classic approach of expert system development. The classical approach does not cover all aspects of complex procedures, one of which is to assess the safety with using of a variety of influence factors.

In real life, people often do not think about issues from the perspective of crisp names and numbers. They constantly have to deal with a wide range of uncertainties. This also applies to experts (or specialists) when they are solving different problems [8]. As it is known in practice, the subjective judgments of experts produces better results than objective manipulation of inexact data [9].

Experts in the field of information security usually operate with fuzzy terms such as "sensitiveness" (for applying of information), the "completeness" (e.g., regarding the CV of the applicant), and etc. To handle uncertainties like mentioned above, we apply one of the approaches of artificial intelligence theory - fuzzy sets and logic theory, as the most effective tool for approximate reasoning in comparison with traditional methods.

Fuzzy inference methods are used in risk assessment theory (as described in [10]). This theory relates to great values of uncertainties. We suppose that the use of fuzzy set theory therefore can be justified in the case of consideration the audit review process to ensure management of information security risks.

In the field of information security, where human involved, such kind of things like “perception” takes place. For example, the auditor may request the user (customer) information about the password change issues by asking the question like "How often do you change your password?" He does not expect such answers as "frequent" or "rarely" because human perception usually differs. Furthermore, the user may have distorted the concept of information security. In this case, the auditor perception is the most adequate. The numeric value (e.g., the number of password changes per month) would be an absolute, independent, and therefore a more sufficient answer in this case. Fuzzyfication is performed on expert’s side. He decides whether the answer is "often", "rarely", and etc.

We can show that fuzzy logic and sets approach is advantageous here and the need of fuzzy logic is going to be proved in this paper.

IV. Methodology of Expert System

Let us highlight the factors that play a key role in information security assessment [1, 4, 11]:

- vulnerabilities: any weaknesses in the system of controls that might be exploited by threats;
- threats: generally the people, things or situations that could potentially cause loss;
- impacts: what would be the (in the worst case) effects if some of those threats actually materialized and hit some of organization’s vulnerabilities.

In order to achieve a qualified security assessment, the auditor should consider each of these categories. We decided to follow their thinking patterns and define the organization's assets, vulnerabilities which may hit assets, and the threats that may be a cause of particular harm. As well we should take into account the implications of the threats.

The following scheme (Figure 1) outlines these categories that are grouped into 3 layers. Some of the samples of each category will be discussed further.

There are two types of assets: physical assets (such as computers, servers, etc.) and information (e.g., employee data, customer data that is stored in the database, etc.). They must be protected (see Standard ISO / IEC 27002, chapter 7.1.1, "Inventory Assets"). Each of the assets has one or more vulnerabilities that it may have. Vulnerability is influenced by several factors (white boxes in the 2nd layer, see Fig.1) and may be caused by particular threat(s) which are exercised with some possibility.

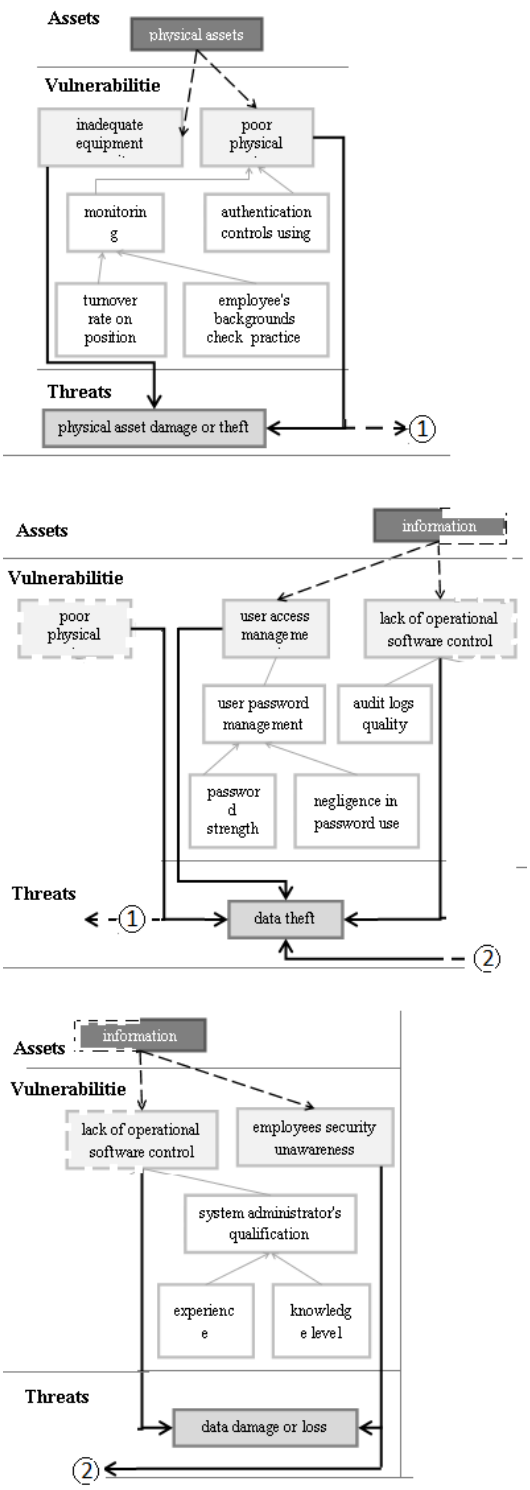

Figure 1 Audit scheme

For example, physical security weakness, such as poor physical entry control (see ISO / IEC 27002, 9.1.2, " Physical entry controls") depends on proper use of authentication control and appropriate monitoring, which in turn depends on staff turnover of guard positions and verifying of their job requirement compliance.

This deficiency may become a cause of physical asset damage, or sensible information theft, or both.

Due to the fact that the accurately assessment of the possibility of adverse situations is very hard process we need to use fuzzy terms to represent the data and we should take into account the impact of all possible factors and rules.

The impact of the vulnerability on the particular threat is reflected in the rules that may be expressed as a following:

IF the vulnerability seriousness is *sufficiently big*, THEN threat execution possibility is *low / medium / high* (representation of fuzzy variables which are marked italics).

For example (in accordance with ISO / IEC 27002, 9.2, "Equipment Security", 9.1, "Secure areas") we can write the rules:

IF an equipment is *inadequate*, THEN physical asset damage or theft *increases slightly*.

IF physical entry control is *poor*, THEN physical asset damage or theft *increases significantly*.

According to this principle, the number of rules will depend on the number of vulnerabilities that are influenced by certain threat and differentiated by severity.

In order to produce one value the corresponding fuzzy numbers are summed and divided by the maximal numbers and multiplied by quantity (e.g., high fuzzy number).

In order to perform some risk assessment we can also consider the impact of materializing of the threats in money equivalent.

As we know, there is no such thing as "exact" value of risk. Risk assessment is carried out on the imprecisely defined inputs, such as, for instance, the likelihood of the threat that is being exercised against the vulnerability, and the resulting impact from the successful compromise. For example, in [10], such values as Robustness of Security Management System (with values - inadequate, good and excellent) and severity of consequences (category of health harm ranging from 1 to 5) from industrial incidents are taken as inputs, the value of risk (with value of negligible, low, moderate, high and unacceptable) is considered as an output value.

In our expert system, the risk can be calculated in the same way, i.e. as a function from the likelihood of threats that is founded as summation of vulnerabilities impact rates and from the size of possible impact in money equivalent. Thus the risk factors with low-level security can be sorted, and recommendations can be labeled with a special level of requirements.

According to Brander [12], we can use the keywords in expert system recommendation reports like "*must*", *"must not"*, *"required"*, *"shall"*, *"shall not"*, *"should"*, *"should not"*, *"recommended"*, *"may "*and*" optional*" that could be implemented in the fuzzy variables. These keywords can deeply and clearly show the priority of recommendations and the manner of notifications.

Once common methodology is defined, we need to focus on ways to translate the standard's recommendations into rules and to determine what types of input data the system will collect.

V. Knowledge and Input Data Interpretation

In our work, we tried to develop a methodology for knowledge acquisition and interpretation of input data that can be considered as an information gathering from the user for the expert system. In this part of paper we investigate the following issues:

- How the standards' recommendations are interpreted in form of the rules?

- What questions should we ask from the user in order to ensure that these recommendations are properly implemented in the organization?

- What kind of inputs should we take as the answers to these questions?

Let's start from the inputs. The easiest case of input is simple numerical values: for example, employee turnover rate (the percent of employees substituted on a particular position during a month or a year), employee's work experience (in years).

Let us give an example from the standards. “The updating of the operational software, applications, and program libraries should only be performed by trained administrators upon appropriate management authorization” (ISO 27002 12.4.1 “Control of operational software”). To determine whether the organization follows this requirement, the management should be asked: “Are your administrators trained?” But since our goal is to be as objective as it's possible, we can't directly ask such questions from users whose perception of information security, in particular, administrators' competence, may be inadequate. Employee's competence depends on several factors, the most common are experience and professional qualification. So, the question “Are your administrators trained?” could be divided into two questions: “Are the administrators experienced?” and “Do the administrators have an appropriate qualification?” In order to eliminate the factor of the misperception, it's reasonable to transform the first question into form “What is the professional experience (in years) of the administrator?”, so that the system would estimate if the administrator is experienced or not by using fuzzy sets approach. Qualification of the administrator is represented by his/her certificates. Also, some companies practice quality assessment by arranging exams to the employees, for example, multiple choice tests with questions like:

1. When setting permissions in NTFS for an individual's network drive, which option(s) of the following levels do you give a default user?

Answers: Full Control / Modify / Read & Execute / Read / Write.

2. What do administrative shared folder names always end with?

Answers: # / $ / @ / % / ~

3. Which one of the following is equal to 1 kilobyte (KB)?

Answers: 512 bytes / 1000 bytes / 1024 bytes / 1028 bytes / 2048 bytes.

4. etc.

The score of multiple choice tests like this could also serve as fuzzy variable and affect the inference. A sample of the fuzzy rule which is used to ensure that employees are on the appropriate position (e.g. system administrator) and enough competent:

IF an employee is experienced *enough* AND the test score is *high*, THEN the employee is *sufficiently* competent ”.

Since multiple choice tests are so convenient way for obtaining information from the user, we decided to apply them in many others aspects of security, for example, user security awareness evaluation (ISO/IEC 27002 8.2.2, “Information security awareness, education, and training”).

Sample questions which may be given to particular users group:

1. Mark a true statement:

- Leaving a terminal logged in is a bad security practice; (correct)
- Frequent logging in and logging out leads to computer hardware fast deprecation;
- Logging out when leaving a work place is a good corporate culture indicator;
- Constantly logging in and out is time consuming.

2. What do you think about using a personal laptop on a workplace instead of a corporate one?

- I think purchasing laptops for employees is a reasonable expense for the company; (correct)
- Laptops are expensive;
- Using a personal laptop is convenient;
- Personal laptop is a secure decision.

Security awareness index could be calculated as an average score for the test or a net (total) score, which gives an overall impression of a particular users' group security education. This index is also treated by our system as a fuzzy variable.

Continuing an issue of a transformation of standards' recommendations into rules and questions, let us introduce another example. ISO/IEC 27002 "Password use" (chapter 11.3.1):

"All users should be advised to:

a) keep passwords confidential;

b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;

c) change passwords whenever there is an indication of possible system or password compromise;

d) select quality passwords with sufficient minimum length which are:

- easy to remember;
- not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;
- not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);
- free of consecutive identical, all-numeric or all-alphabetic characters;

e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

f) change temporary passwords at the first log-on;

g) not include passwords in any automated log-on process, e.g. stored in a macro or function key;

h) not share individual user passwords;

i) not use the same password for business and non-business purposes."

These guidelines reflect two sides of the security: technical (password quality) and human-behavioral aspect (how carefully user manages his/her passwords). We will look at them separately and define two fuzzy variables: password strength and user negligence level in password managing (that is performed by a number from 0 to 1) which may have corresponding possible values: weak, good, strong - for password strength and low, moderate, high – for user negligence level. One sample of fuzzy sets for Password Strength can be demonstrated on Figure 2.

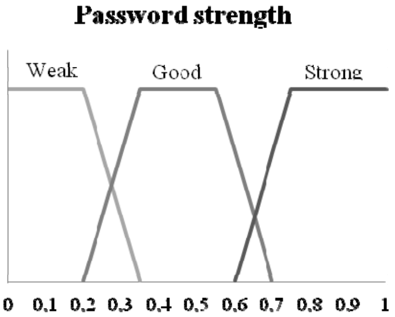

Figure 2: A sample of fuzzy set for password quality variable.

Depending on two values that are mentioned above, we can make a conclusion about a possibility of unauthorized access to company's system (see table 1).

Table 1: A relationship between password quality, user's negligence and possibility of unauthorized access.

Negligence \Strength	weak	good	strong
low	M	H	H
moderate	L	M	H
high	L	L	M

On the base of table 1 we can compose fuzzy rules as a following:

IF negligence is *low* and password is *strong*, THEN the password security is *high*.

IF negligence is *low* and password is *good*, THEN the password security is *high*.

IF negligence is *low* and the password is *weak*, THEN the password security is *moderate*.

IF negligence is *moderate* and password is *strong*, THEN the password security is *high*.

IF negligence is *moderate* and password is *good*, THEN the password security is *moderate*.

IF negligence is *moderate* and the password is *weak*, THEN the password security is *low*.

IF negligence is *high* and password is *strong* THEN the password security is *moderate*.

IF negligence is *high* and password is *good*, THEN the password security is *low*.

IF negligence *high* and password is *weak*, THEN the password security is *low*.

The rules above define the quality characteristics of fuzzy numbers. Now we should consider how to calculate the inputs by performing them as a numeric value.

We tried to compose two questions to determine the numeric values of fuzzy numbers. First question is about how user manages passwords, and the second one defines password quality. Each of the points in the question has a weight, the total score for the question (and the input for fuzzy variable) is found as a sum of the weights of marked items. Near each question we specify the fuzzy number from fuzzy set ranging from 0 to 1.

The first question: Mark points you think are true for you:

- My colleagues/family members/friends or somebody else know my password :0.2
- I consider writing down my logins and passwords on paper, storing them in files, or let my browser remember them very convenient way not to forget my passwords. :0.15

- If something suspicious happens, I don’t think it is necessary to immediately change my password. :0.15

- I don’t change my password without any serious reason, my memory is not so good to remember new password. :0.1

- I think a default password is fairly strong. :0.25

- I use same password in multiple services. :0.15

The second question: My password usually:

- is difficult to remember

- is a default password, like password, default, admin, guest, etc. :0.2

- contains dictionary words, like chameleon, RedSox, sandbags, bunnyhop!, IntenseCrabtree, etc. :0.1

- consists of words with numbers appended: password1, deer2000, john1234, etc. :0.15

- is one of common sequences from a keyboard row: qwerty, 12345, asdfgh, fred, etc. :0.3

- contains personal information, like name, birthday, phone number or address. :0.15

- contains symbols such as (mark each):

- Lowercase letters (26), Uppercase letters (26), Numbers (10), Punctuation marks (5)

- has average length: (specify number of characters)

- (not an option: using 2 previous options number of possible combinations of characters is calculated as (summary number of symbols)^(length); coefficient for this question is 0.1 if combination is bigger than 10^12, and combinations number / 10^12 * 0.1 otherwise)

Since we defined questions for each variable and rules we can calculate possibility of unauthorized access.

Ways to obtain particular variable’s value, mentioned above, are focused on retrieving numerical values. But sometimes it is not enough for producing a good result. For example, risk assessment field contain a great value of uncertainties and fuzziness. There is no such thing as exact value of the risk; impacts of exercising particular threats, especially in information security field, are very difficult to calculate. We consider efficient to have user defined fuzzy sets as the inputs to those impacts. E.g. user may specify value *about 10000$* as the answer for the question: “What would be a possible loss (in money equivalent) if some malicious person broke-in to company’s system?”

Fuzzy sets and logic approach gives an ability to efficiently handle imprecision and uncertainties, in environment of which humans successfully operate [10]. Furthermore, fuzzy expert systems allow writing rules in almost natural language, what simplifies an interaction between knowledge engineer and domain expert [8].

VI. Conclusion

The closer to human expert behavior of the system is obtained, the more effectively it is able to perform the task it was made for. Fuzzy expert system applied in information security field is sufficient technique for emulating specialist’s decision-making ability.

Theoretical significance of this work has been presented in publications before [13, 14]. This paper is actually part of whole scientific research, touched approaches and several issues of implementing fuzzy logic in problems of information security auditing and development of fuzzy expert systems.

In summary, we can highlight the fact that these studies including development of expert systems will engage several research areas of implementing of fuzzy neural networks and neural algorithms in the self-learning expert systems.

In conclusion, we can claim that there are enough untouched areas and bright intersections at the implementing expert systems in security auditing, in development of fuzzy knowledge base, in the integration of fuzzy coefficients for security auditing recommendation reporting, and etc.

We can suppose that these research directions may become a good scientific foundation in development of artificial intelligence.

References

[1] Hinson, G. 2008. Frequently Avoided Questions about IT Auditing. Available: http://www.isect.com/html/ca_faq.html

[2] Val Thiagarajan, B.E. 2002. BS 7799 Audit Checklist. Available: www.sans.org/score/checklists/ISO_17799_checklist.pdf

[3] ISO IEC 27002 2005 Information Security Audit Tool. Available: http://www.praxiom.com/iso-17799-audit.htm

[4] Stepanova, D., Parkin, S. and Moorsel, A. 2009. A knowledge Base For Justified Information Security Decision-Making. In 4th International Conference on Software and Data Technologies (ICSOFT 2009), 326–311.

[5] Giarratano, J., and Riley, G. eds. 2002. Expert Systems: Principles and Programming. Reading, Mass.: PWS Publishing Company.

[6] Tsudik, G. and Summers, R. 1990. AudES - an Expert System for Security Auditing. IBM Los Angeles Scientific Center.

[7] Zadeh, L. 1994. Fuzzy Logic, Neural Networks, and Soft Computing.

[8] Siler, W., Buckley, J. eds. 2005. Fuzzy Expert Systems and Fuzzy Reasoning. Reading, Mass.: Wiley-interscience.

[9] Borjadziev, G., Borjadziev, M. eds. 1997. Fuzzy Logic for Business, Finance, and Management. Reading, Mass: World Scientific.

[10] Mahant, N. 2004. Risk Assessment is Fuzzy Business—Fuzzy Logic Provides the Way to Assess Off-site Risk from Industrial Installations. Bechtel Corporation.

[11] Elky, S. 2006. An Introduction to Information Security Risk Management. SANS Institute.

[12] Bradner, S. 1997. Key words for use in RFCs to Indicate Requirement Levels. IETF RFC Repository. Available: http://www.ietf.org/rfc/rfc2119.txt?number=2119

[13] L. Atymtayeva, A. Akzhalova, K.Kozhakhmet, L. Naizabayeva. 2011. Development of Intelligent Systems for Information Security Auditing and Management: Review and Assumptions Analysis. Proceedings of the 5th International Conference on Application of Information and Communication Technologies, 12-14 October, 2011, Baku, Azerbaijan, pp.87-91

[14] K. Kozhakhmet , L. Atymtayeva. 2011. Creation of Concept an Innovative universal platform of virtual computing systems for scientific problems solving. Proceedings of the 9th INTERNATIONAL CONFERENCE: INFORMATION TECHNOLOGIES AND MANAGEMENT 2011, April 14-15, 2011, Information Systems Management Institute, Riga, Latvi, p.96