Krassimir Markov, Vitalii Velychko,
Lius Fernando de Mingo Lopez, Juan Casellanos
(editors)

# New Trends in Information Technologies

I T H E A
SOFIA
2010

Krassimir Markov, Vitalii Velychko, Lius Fernando de Mingo Lopez, Juan Casellanos (ed.)

New Trends in Information Technologies

ITHEA®

Sofia, Bulgaria, 2010

ISBN 978-954-16-0044-9

First edition

Recommended for publication by The Scientific Concil of the Institute of Information Theories and Applications FOI ITHEA

This book maintains articles on actual problems of research and application of information technologies, especially the new approaches, models, algorithms and methods of membrane computing and transition P systems; decision support systems; discrete mathematics; problems of the interdisciplinary knowledge domain including informatics, computer science, control theory, and IT applications; information security; disaster risk assessment, based on heterogeneous information (from satellites and in-situ data, and modelling data); timely and reliable detection, estimation, and forecast of risk factors and, on this basis, on timely elimination of the causes of abnormal situations before failures and other undesirable consequences occur; models of mind, cognizers; computer virtual reality; virtual laboratories for computer-aided design; open social info-educational platforms; multimedia digital libraries and digital collections representing the European cultural and historical heritage; recognition of the similarities in architectures and power profiles of different types of arrays, adaptation of methods developed for one on others and component sharing when several arrays are embedded in the same system and mutually operated.

It is represented that book articles will be interesting for experts in the field of information technologies as well as for practical users.

General Sponsor: Consortium FOI Bulgaria (www.foibg.com).

Printed in Bulgaria



**ISBN 978-954-16-0044-9**

C\o Jusautor, Sofia, 2010

# METHODS OF ANALYSIS FOR THE INFORMATION SECURITY AUDIT

**Natalia Ivanova, Olga Korobulina, Pavel Burak**

***Abstract**: In this article authors propose the analysis of the main information security audit methods: the active audit, the expert audit and the audit on conformity with standards applying SWOT-analysis. After this analysis authors make the suggestions for the future work in this area.*

***Keywords**: information security, audit, threat, vulnerability, audit method, SWOT- analysis.*

## Introduction

Information systems play an important role in our life. There is a big amount of important information flows that should be protected from unauthorized access and unauthorized modification. The information security systems are designed for the critical information protection.

The information security system is a complex of organizational, technical and legal measures that are used to protect information from unauthorized access and unauthorized modification in the process of receiving, processing, storage and transmission.

The information security systems correctness must be checked continuously to maintain the required security level. The information security audit is for this purpose.

The Information security audit is necessary for identifying the gaps in information security systems and, on the basis of the results, improving their protective functions. If the information security systems defense functions are not revealed in time, they may possibly cause the leak of confidential information which would adversely affect the information system image and would reduce the users' trust in it.

## The information security threats classification

The Information security means maintaining the information confidentiality, integrity and availability and also the information authentication, the system reliability, control over the commitments' implementation [Standard, 2005]. Standard [Standard, 2005] also introduces two important definitions: the definition of the information security threats and the information security vulnerabilities. The threat is a potential cause of an undesirable incident, which may cause harm to the information system or the company. Vulnerability is a negative feature of an asset or a group of assets, through which one or more threats can be implemented. Thus, the information security may be compromised as a result of the information security threats, which are implemented through the vulnerabilities that exist in the information system.

All the information security threats can be classified, and today there are many different classifications. The authors of this research present a proper information security threats classification that is illustrated in figure 1. Table 1 presents all threats in order and each threat gets its own number. The main vulnerabilities for these threats are presented in table 2.

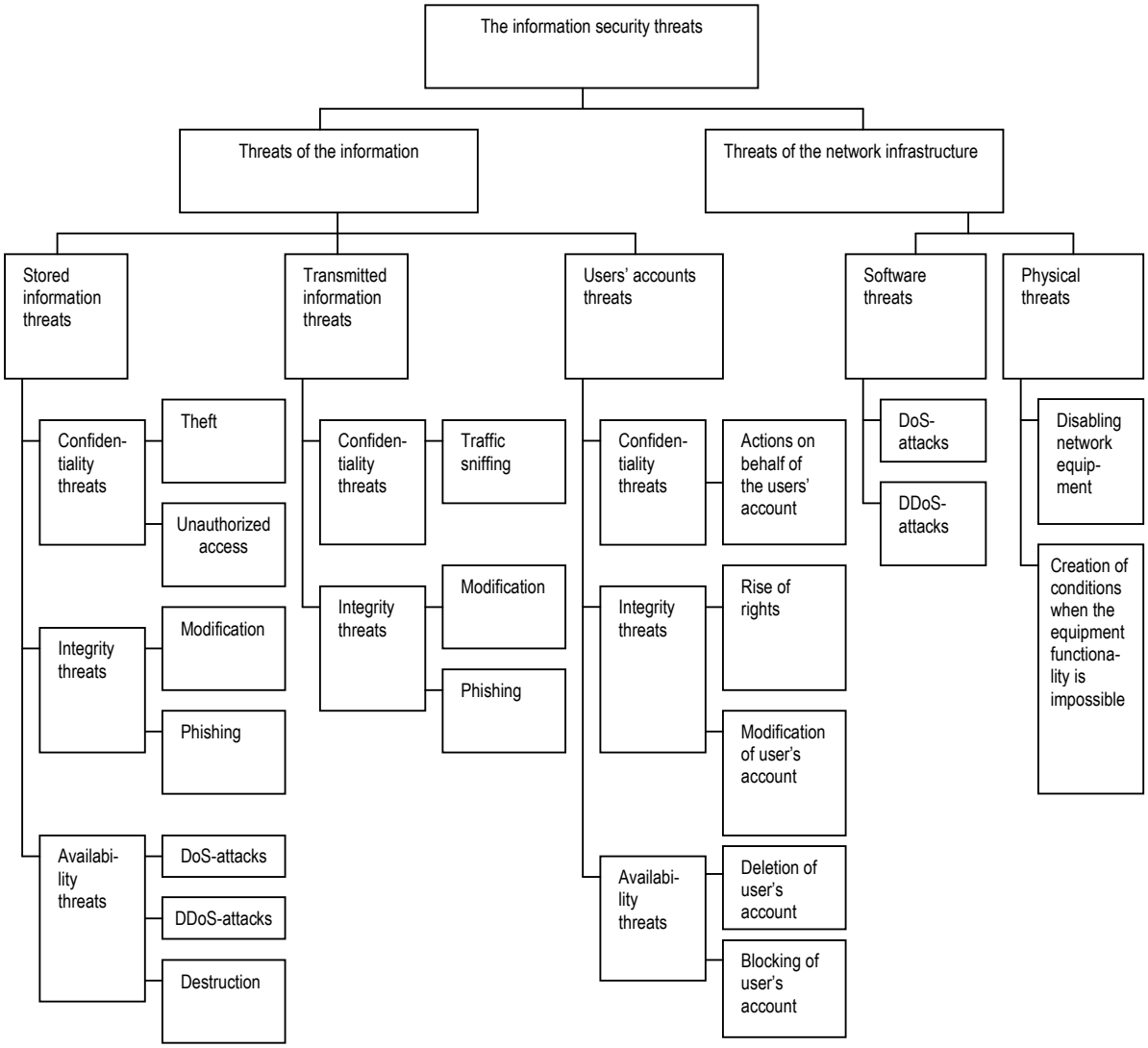


**Figure 1 – Threats classification.**

**Table 1 – The list of threats.**

| № | The threat name |
|---|---|
| 1 | The stored information theft |
| 2 | Unauthorized access to the stored information |
| 3 | The stored information modification |
| 4 | The stored information phishing |
| 5 | DoS-attacks |
| 6 | DDoS-attacks |
| 7 | The stored information destruction |

| | |
|---|---|
| 8 | The traffic sniffing |
| 9 | The transmitted information modification |
| 10 | The transmitted information phishing |
| 11 | The transmitted information destruction |
| 12 | Actions in the system on behalf of the authorized user (masquerade) |
| 13 | The rise of rights |
| 14 | The users' accounts modification |
| 15 | The users' accounts deletion |
| 16 | The users' accounts blocking |
| 17 | The network equipment disabling |
| 18 | Creation of the conditions when the equipment functionality is impossible |

**Table 2 – The list of vulnerabilities.**

| **Vulnerability** | **The ongoing threats numbers** |
|---|---|
| The weak cryptographic policy | 2, 3, 8, 9 |
| The firewalls invalid configuration | 1, 2, 4, 5, 6 |
| The weak password policy | 12, 14 |
| Lack of check-point in the company | 1, 17, 18 |
| Harmful effects on the lines of force outside the company | 11, 18 |
| Disasters | 11, 17, 18 |
| Free access to communication channels outside the company | 8, 10, 11 |
| The incorrect implementation of the restricting access rules to the stored information | 1, 2, 3, 4, 7 |
| The intrusion detection systems and the intrusion prevention systems incorrect work | 1, 2, 4, 5, 6, 7 |
| The antivirus software incorrect configuration | 3, 7, 9, 14, 15, 16 |
| The use of unprotected data transfer protocols | 8, 9, 10, 11 |
| The users' rights incorrect settings | 12, 13, 14, 15, 16 |
| The integrity check mechanisms' incorrect settings | 3, 9, 14 |
| Uncontrolled technical channels of information leakage | 8, 10, 11 |
| The restrictions absence on the number of logon attempts | 1, 2, 12 |

## The information security methods

The information systems audit and control association (ISACA) provides the following definition to the term "the information security audit":

The information security audit is a process of the information gathering and the information analysis in order to establish:

- weather the organization's resources (including data) security is provided;
- whether the necessary parameters of the data integrity and the data accessibility are provided;
- are the organization's goals in the terms of the information technologies effectiveness reached.

Today there are three main the information security audit methods. They are presented in figure 2.

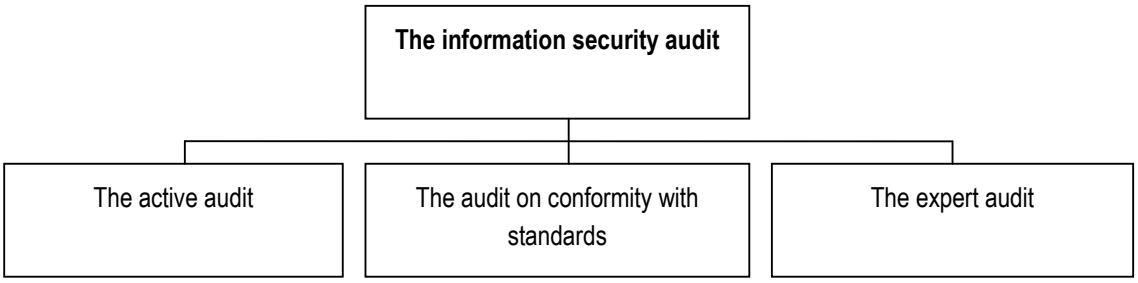


Figure 2 – The information security audit methods.

The information security active audit is a study of the information system information security from the perspective of a hacker or cracker who is highly skilled in information technologies [Prosyannikov, 2004].

During this audit method a large number of network attacks that hacker can implement is modeled. The same conditions in which the hacker works are artificially created for the auditor. The auditor is also provided only that information that can be found in open sources. The active audit result is the information about all the vulnerabilities, their severity degree and their elimination methods.

The expert audit is the information security comparison with the "ideal" description, which is based on:

- the CIO requirements;
- the "ideal" security system description based on accumulated in the audit company the worlds' and the private experience [Prosyannikov, 2004].

The performed during the expert audit actions are presented in figure 3.

The method of interviewing employees is used to collect the initial information. Technical specialists answer the questions related to the information systems operation, and the company's management explains the requirements that are applied to the information security system. The expert audit results can contain various proposals about modifying or upgrading the information security system.

During the audit on conformity with standards the information security state is compared with some abstract description found in the information security standards [Prosyannikov, 2004]. The information security standards are presented in figure 4.

The reasons for the audit on conformity with standards (and certification) may be divided into 4 categories, depending on the necessity of this service for the company:

- Compulsory certification;
- Certification due to the external objective reasons;
- Certification, which allow getting the benefits in the long term;
- Voluntary certification.

After this audit method the official report is generated. It contains the following information:

- The extent to which the information system matches selected standards;
- The extent to which the information system matches the company's' internal information security requirements;
- The number (and the categories) of disparities and received comments;
- Proposals about modifying or upgrading the information security system to bring it to conformity with standards;
- Detailed references to the company's key documents, such as security policies, descriptions of not obligatory standards and norms, applicable to the company.

Nowadays an increasing number of companies consider the certification as the confirmation of the high level information security. They use the received certificates as a "trump card" in the fight for a major client or business partner.

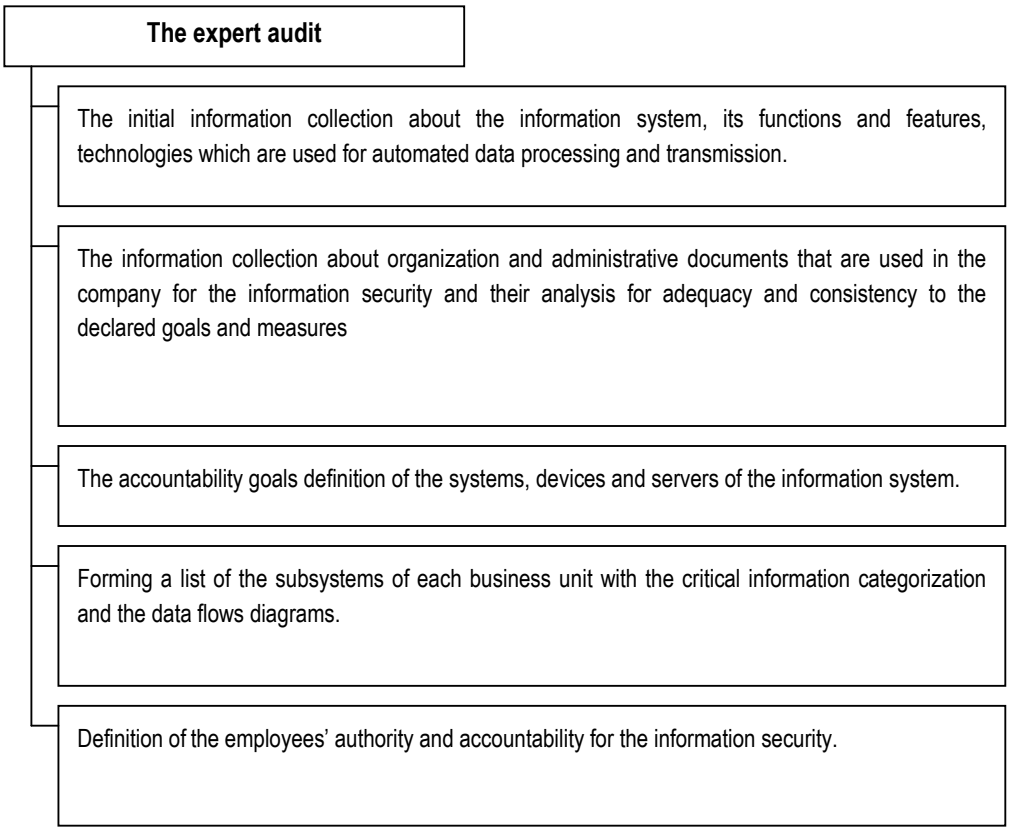


Figure 3 – The expert audit.

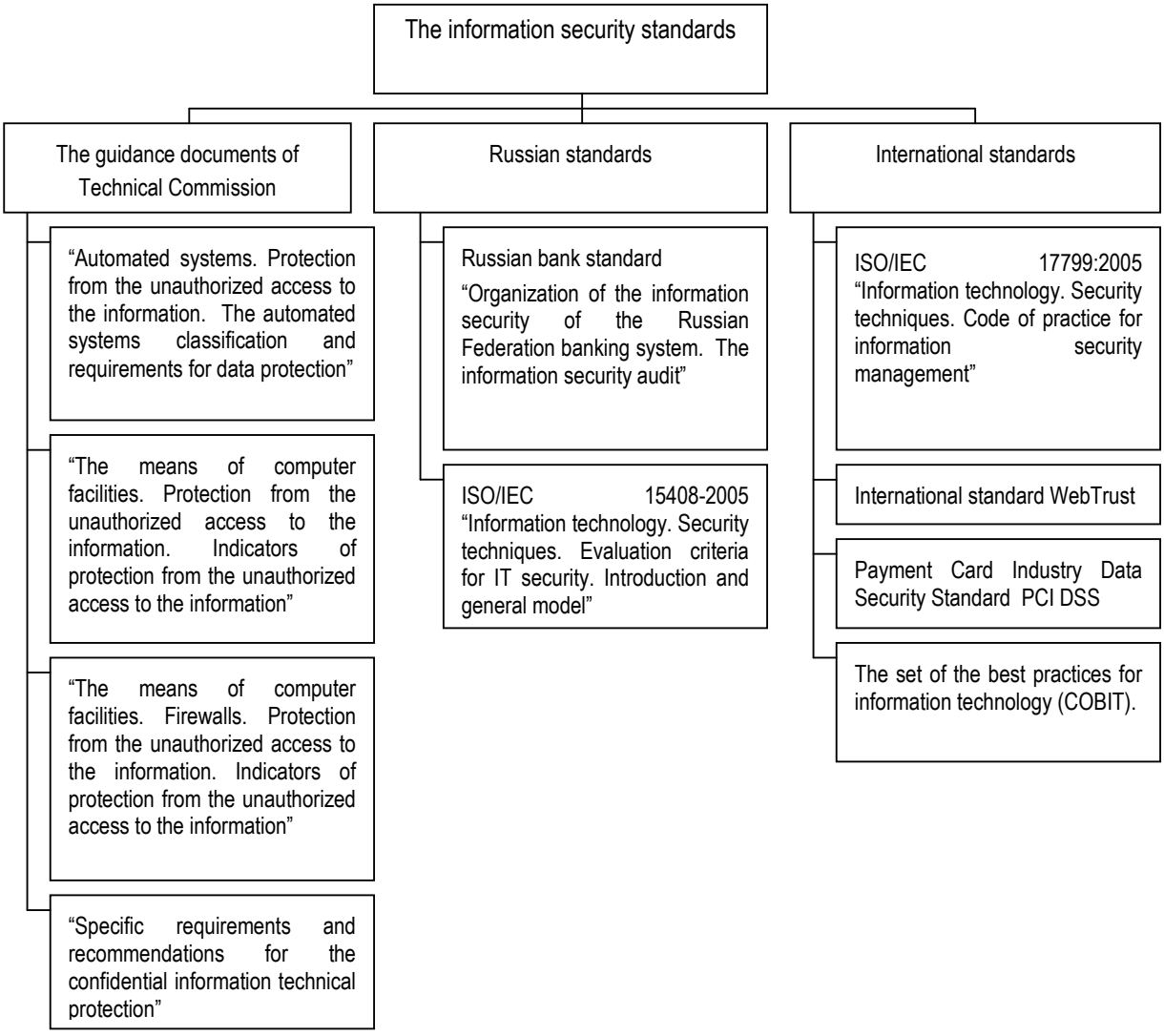


**Figure 4 – The information security standards.**

## The audit methods analysis

The useful tool for the information security audit methods analysis is SWOT-analysis.

Initially, SWOT-analysis was created for different marketing researches but its mechanism is quite universal so the SWOT-analysis can be applied in other areas. SWOT-analysis aim is to determine the company's strengths and weaknesses (the internal environment analysis), as well as opportunities and threats of the nearest company's environment (the external environment analysis) [Gvosdenko, 2006]. The SWOT-analysis results are used to plan the company's strategy.

In this paper SWOT-analysis is used to determine the strengths and the weaknesses of the information security audit methods, as well as to identify external factors that are able to make the audit procedure easier or, on the contrary, more complicated.

Using the SWOT-analysis results, we can decide which audit method is the most perspective and how it is possible to develop its development strategy.

Tables 3, 4 and 5 represent the information security audit methods SWOT-matrixes.

**Table 3 - The active audit SWOT-matrix.**

| Strengths | Weaknesses |
|---|---|
| The audit process automation.<br>The audit doesn't require the employees' participation.<br>The audit frequency is not regulated.<br>It is possible to carry out the stress test in order to determine the system productivity and stability, as well as the system resistance to DoS-attacks. | The additional software is required.<br>Users should stop working with the information system before the audit beginning.<br>Audit can identify only the known vulnerabilities. |
| **Opportunities** | **Threats** |
| High demand in the market.<br>Audit can be carried out by the information security department staff.<br>There is a large number of different software from various organizations.<br>The biggest part of the auditors' work is automated. | The necessary software is expensive.<br>Each system requires different software.<br>The software can contain errors.<br>There are no laws for this audit method. |

**Table 4 - The expert audit SWOT-matrix.**

| Strengths | Weaknesses |
|---|---|
| The additional software is not required.<br>Users may work with the information system during the audit.<br>The audit frequency is not regulated.<br>The audit is based on the information security threats, thereby it is possible to cover a large number of vulnerabilities. | The employees should participate in the audit.<br>The information provided by the client company should be precise.<br>Preparative works can last long.<br>The audit may occupy a considerable amount of time. |
| **Opportunities** | **Threats** |
| A big accumulated experience of the expert knowledge in the information security field.<br>There are necessary regulatory documents.<br>Audit can be carried out by the information security department staff.<br>It is possible to atomize the audit process. | The absence of the audit process automation means.<br>The need to trust the expert estimates.<br>High requirements for the experts' competence.<br>Potential conflicts among the experts' opinions. |

**Table 5 - The audit on conformity with standards SWOT-matrix.**

| Strengths | Weaknesses |
|---|---|
| The audit carrying out is regulated by normative documents.<br>The reports' structure is described in the normative documents.<br>Additional software is not required.<br>Users may work with the information system during the audit. | The employees should participate in the audit.<br>The audit should be carried out after every change in the information system.<br>The information provided by the client company should be precise.<br>The audit may occupy a considerable amount of time. |
| **Opportunities** | **Threats** |
| The security certificate, issued after the audit, raises the company's prestige.<br>The best expert practices are reflected in the normative documents requirements.<br>High demand in the market. | A large number of the normative documents.<br>Constant changes in the normative documents.<br>The contradictions in the normative documents.<br>The audit can't be performed by the company itself, because the security certificate is issued only by the accredited organizations. |

In order to pass from the qualitative estimations to the quantitative ones, for all the factors listed in tables 3, 4 and 5 the authors identified the following values:

- The rate of the factor importance (F_impi);
- The observed value of the factor impact (F_infi);
- The uncertainty of judgments (F_probi).

The significance of each factor is calculated by the formula:

$$F\_val_i = F\_inf_i * F\_prob_i \quad (1)$$

Then the total significance of all the factors for each parameter is as follows:

$$Val = \sum_{i=1}^{n} F\_imp_i * F\_val_i \quad (2)$$

The calculation results for each information security audit method are presented in table 6. Figure 5 illustrates the obtained values by the histogram.

Table 6 – The **parameters'** significance.

| | The active audit | The expert audit | The audit on conformity with standards |
|---|---|---|---|
| Strengths | 112,75 | 137,15 | 98,70 |
| Weaknesses | 147,20 | 147,00 | 154,35 |
| Opportunities | 174,80 | 184,95 | 163,80 |
| Threats | 165,45 | 181,70 | 184,40 |

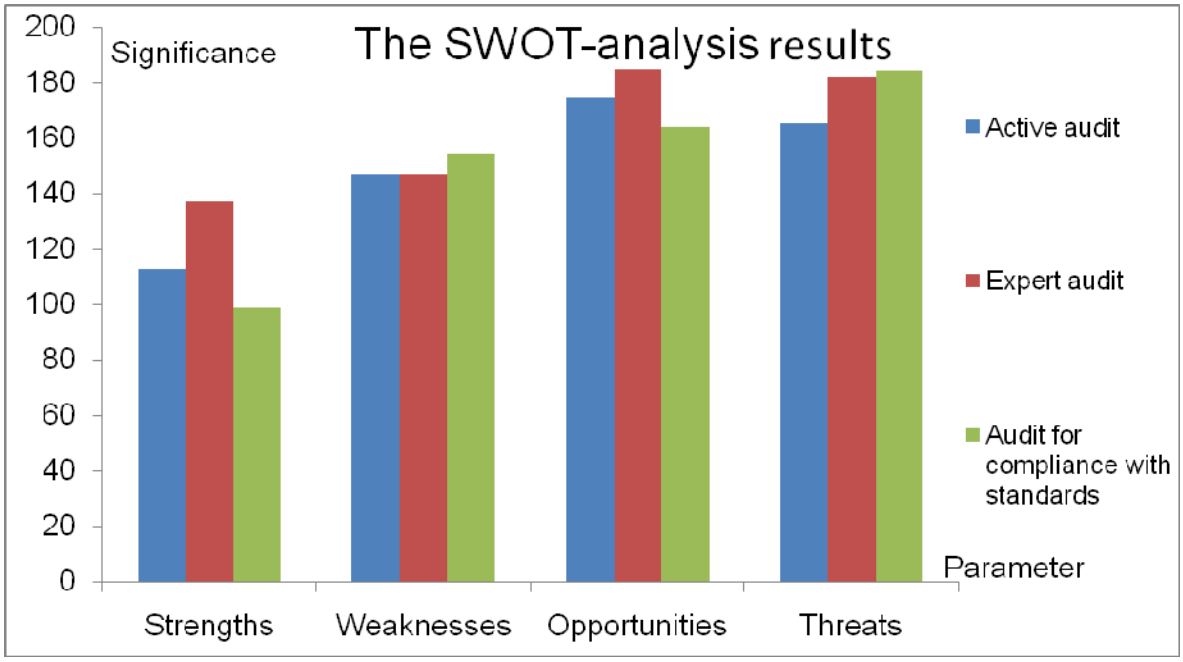


Figure 5 – The SWOT-analysis results.

From the table 6 and the histogram in figure 5 it is clear that expert audit has the best results. Consequently, this method is the most perspective information security audit method.

The expert audit requires good trained experts, but there are not many specialists of such a level. In addition, the task is poorly formalized and is based on the experts' personal experience and intuition. In this regard, we can conclude that in order to solve these problems we should use an expert system based on knowledge.

## Conclusion

Information systems work with important and sometimes even critical information. This information should be protected from the unauthorized access and the unauthorized modification, to avoid harmful incidents. The information security systems are created for this purpose. Their correctness should be checked regularly, in order to maintain the demanded security level. The information security audit is the process that does this check. It is the difficult process demanding the knowledge of highly skilled experts. So in this case authors create the expert system which could help to make this difficult but very important and critical work.

## Bibliography

[Standard, 2005] ISO/IEC 17799 2005 "Information technology. Security techniques. Code of practice for information security management"

[Prosyannikov, 2004] R.Prosyannikov. To get rid of errors: the information security audit methods. In: "Connect! The word of connection", №12/2004.

[Gvosdenko, 2006] A. Gvosdenko. SWOT-analysis: methods of carrying out and application possibilities in the Russian enterprises. In: "Marketing and marketing researches", №2/2006.

## Authors' Information

***Natalia Ivanova*** *– Ph.D.(Tech), Associated Professor of Petersburg State Transport University, department of Informatics and Information safety*

*190031, Russia, Saint-Peterburg, Moskovskij prospect, 9*

*e-mail: natali_iv@rambler.ru*

***Olga Korobulina*** *– Post Graduate Student of Petersburg State Transport University, department of Informatics and Information safety*

*190031, Russia, Saint-Peterburg, Moskovskij prospect, 9*

*e-mail: Olga_korobulina@list.ru*

***Pavel Burak*** *– Petersburg State Transport University, department of Informatics and Information safety*

*190031, Russia, Saint-Peterburg, Moskovskij prospect, 9*

*e-mail: wistle3b@gmail.com*