Building a Knowledge Base for Expert System in Computer and Information Security

Vishal Srivastava, Rehan Farooque
Department of Computer Engineering
vishalsrivastava8630@gmail.com, rehan16071999@gmail.com

Abstract. - In the days of technological advancement, a role of computer and its information security (IS) is very important. There is an urgent need in implementing and assessing information security at a good level. However, it is accompanied with very high costs: experts in IS are quite expensive specialists. An automation of some security implementation and evaluation tasks can reduce these costs and potentially increase the quality of IS strategies being developed and IS audit quality. We believe that expert systems approach can be beneficial in achieving this automation. Though information security is a very broad field, encompassing many complex concepts, we are trying to develop a methodology of formalizing of IS knowledge to build a knowledge base for expert system that can serve as IS audit expert. In this paper we discuss methods for knowledge base building.

Keywords: Key-Words: - expert systems, information security, Computer Security, knowledge base

• Introduction

Nowadays it is almost impossible to find a branch of human activity where there is no information technology (IT). Because of IT technologies rapid growth the companies often encounter with the need of increasing the information security. However, information security is a comprehensive system that is very difficult to manage. As a consequence, in the most organizations there is a risk of the information system safety.

The best solution in these circumstances may become the audit of the information security in organizations. The audit process is highly expensive in terms of time and cost as well as in the degree of involvement of human resources.

One of the efforts taken in reducing expenses and facilitating audit is the use of special tools such as checklists and questionnaires, to identify gaps between certain security standards and existing organization's security practices. ISO 17799 Checklist ([1]) provides number of audit questions regarding ISO standard

guidelines. ISO IEC 27002 2005 (17799) Information Security Audit Tool, described in [2], offers several hundred audit questions (questions are stated in yes-no form), pointing to security practices that need to be implemented and actions that should be taken (in case of "no" answer to question). Though these tools cannot be used independently, without any additional security measurements, they still are useful for human auditors. Thus, auditing process can be seen as a process of asking questions and making conclusions from answers.

Another effective tool for the audit is to develop a knowledge base that will pro- vide information for Chief Information Security Officers (CISOs) and will help them to find the right management decisions on the information security policy [3]. 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 the compo- nents and issuing recommendations. As a result, the so-called meta-model of the secu- rity standard recommendations could be constructed[4-7].

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 com- puter analysis of the situation and issuing guidelines and recommendations.

We think that expert systems have much to offer in the case of IS audit automation. Expert systems (ES) approach firstly fits question-answer format of auditing, secondly, ES function on the basis of meta-model that reflects knowledge in target field.

Emulating the way expert in particular field thinks and implementing common human logic can give a system that is able to assess the situation and make decisions.

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 [8].

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 real- ize) remains largely untouched. Our task is to study and solve the problems of devel- opment of expert systems in a wide range of information security audit, which in- cludes aspects of computer security.

In the process of the development of the ES in IS, we passed the following stages:

- Building a high-level structure of the knowledge base for IS. This stage encom- passes analyzing IS standards and deriving key concepts from them; formalizing a process of IS assessment and decision-making.
- Development of system workflow. At this stage, we developed a model where all parts of our system (key elements, identified on the previous stage) can nicely play together [4-5].
- Developing a methodology for population of the knowledge base. The stage in- volves deriving lower-level concepts and subconcepts.

In this paper, we focus on the last stage, but for good understanding it's necessary to stop at the previous two.

• Knowledge Base Structure and System's Workflow

The aim of the expert system's knowledge base is to represent domain specific knowledge in the form which can be used by a computer to effectively operate on this knowledge. In order to meet this requirement, we have chosen to build ontology (knowledge model) of information security domain. Our ontology consists of 4 main entities and relationships between them.

The ontology is divided into two parts: the concepts representing IS domain know- ledge (which actually are core concepts of the domain) and the concepts representing concrete information about considered organization, which are essential in measure- ment of its security level. These concepts are:

-Threat is a potential cause of an unwanted incident, which may result in harm to a system or organization [ISO].

-Vulnerability is a physical, technical or administrative weakness which could be exploited by threats.

-Control concept is used to mitigate vulnerabilities by implementing either organi- zational or physical measures.

-Asset is anything that has value to the organization [ISO]. Also assets are used to implement controls.

The most important relations between these concepts are:

-Threat threatens asset.

-Vulnerability is exploited by threat Severity.

-Vulnerability is mitigated by control.

-Control is implemented by asset Effectiveness.

-Asset has vulnerability.

This is a short explanation of main components of our knowledge model, on top of which we build a knowledge base. We also develop a methodology of risk assessment using the concepts and relations in the knowledge base [1].

The next our step was to determine how our system uses described knowledge model to assess information security level in given organization. In a nutshell, our system asks the user (a person responsible for security, organization's management or company's employees) a set of questions of various forms, analyzes the answers to questions using its knowledge base, and calculates security risks together with giving recommendations for improving security level.
The workflow of our system encompasses the following steps:

- **Collecting enterprise data**

The first stage in the work of our system is collecting data of an organization to be audited. It includes gathering knowledge about assets (everything that need to be pro- tected) and their value to the company.

To achieve this, a variety of question templates is constructed. Basically, the fol- lowing information is expected as an answer to these questions:
-asset (assets) that is (are) presented / not presented;
-and/or value of assets (their attributes);
-the dependencies between the different
assets. Example of possible questions:

Do you have any data centers (asset)? Where they are located? (The possible an- swer may be a plan of company's buildings, which allows revealing dependencies of
the asset on other assets, e.g. a dependency of a data center on the building it is si- tuated in, the building's heating system, fire protection system, etc.) What would be a
loss in case your data center was damaged or destroyed? (The answer should be in money or in per cent equivalent which represent the value ofasset)

We are certain about creating as full and detailed categorization of assets and types of dependencies between them as possible, as it is a key to our results' accuracy. This categorization lays the ground to creation of the set of questions for this stage.

- **Threats, vulnerabilities and controls identification**

After the system has collected all necessary information about the target organiza- tion, it tries to find threats relevant to assets (threats which threaten assets) identified at the previous stage. Then it tries to find vulnerabilities that can exploit these threats and controls that could possibly mitigate these vulnerabilities.

The reason we collect data about these three concepts (asset, threat

vulnerability), besides construction of a complete information security domain ontology, is risk cal- culation. We will explain it in more detail further.

- **Collecting data about organization's security policy and its implementation**

In order to assess the quality of implementation of a control in the target organiza- tion, the system asks several questions regarding each of the standards' control. Each question should identify a value of one variable. For example:

- How often do you perform backups of sensitive data? (The answer to the question is a value of a variable called backup frequency expressed in backups/year)
- How many percent of sensitive information do you usually backup? (The variable is backup coverage in %)

As a concluding phase of the whole process, on the basis of these values and using fuzzy/non-fuzzy rules, a control effectiveness is calculated (i.e. how effective is par- ticular control's implementation in the organization)[9-12].

To be clearer we can summarize above information into the scheme on the figure below (Figure 1).

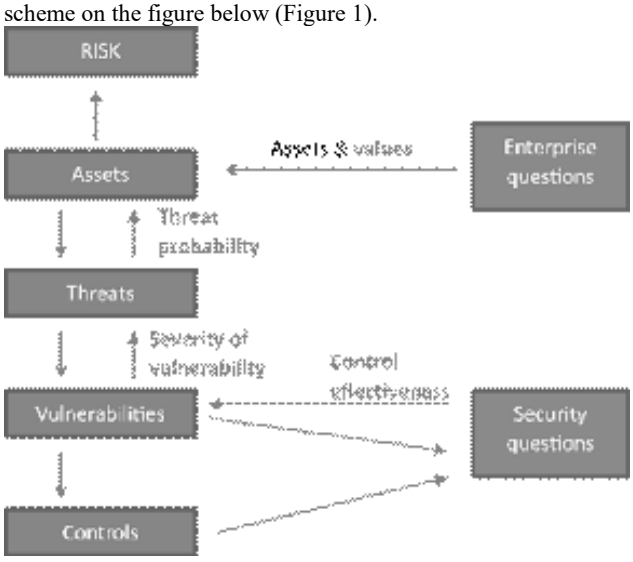


Fig. 1. Scheme of mapping process for all components of ontology

"Enterprise questions" is a set of questions about target organization, the answers to which (list of assets, dependencies, and values of assets) are captured in the very first stage. It results in a populating enterprise part of the knowledge base with asset instances.

The system then finds appropriate threat, vulnerability, control instances and forms new set of questions regarding security practices ("Security questions") in the given company. The answers to these questions allow firstly to calculate control effectiveness of each control, secondly use severity of vulnerability coefficients (pre-

defined) when the threat probability coefficients for each threat can be derived, and, finally, calculate security risks on the basis of latter coefficients and asset values.

However, to make the system working, we need a rich set of objects (concepts' instances) to operate on. We propose using international information security standards (like ISO 27002) for extraction of the knowledge about the field, particularly expressed in a form of elements of our ontology, i.e. instances of 4 concepts and their relationships.

- **The method to collect concepts' instances**

The subjects of information relations (source, the owner, the owner or the user in- formation) define a set of data resources to be protected against various attacks. For assets information systems usually include: material resources, information resources such as analytical, service, control information at all stages of the life cycle: creation, processing, storage, transfer, disposal; Information technology life cycle processes automated systems, providing information services, and etc [13].

The attacks are the result of the threats made through the various security vulnera- bilities, and have a probability (in terms of risk of attack). Main security breaches the following concepts: the disclosure of information values (loss of confidentiality), unauthorized modification to their loss of integrity, or unauthorized loss of access to these values (loss of availability). In the result of analysis of security vulnerabilities, properties, sources of threats such as nature of the occurrence, character and attitude to the objects of Information Systems, and possible probabilities implementation in a particular environment, we can determine risks for given set of information resources [14-18]. This determination allows us to define the security policy. Elaborated subject of information relations strategy of protection may provide for each of the threat the possible line of behavior, namely, the attempt to eliminate the source of the threat; threat avoidance; adoption of threats; minimization of the damage from an attack caused by this

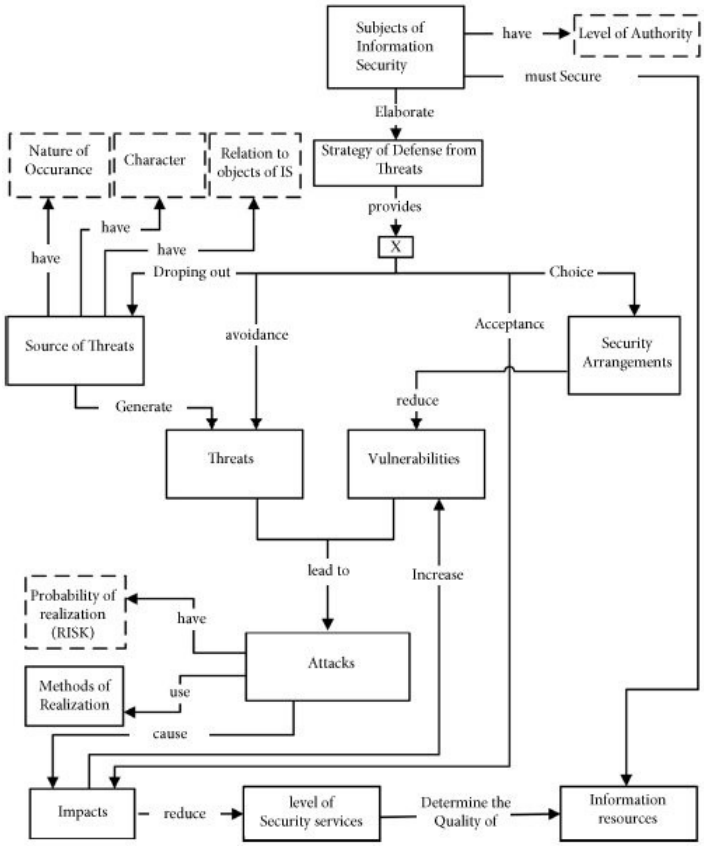
threat by using the services and security mechanisms. It should be taken into account that individual vulnerability can be preserved after use of protective activities [19-21].

Proceeding from the given principles above, we can say that the modeling and classification of the sources of threats and their displays may be carried out by analysis of interaction of logical chains. These logical chains may be constructed by using security policy and analyzing the possible risks.

At the same time the security policy defines a coherent set of mechanisms and security services, adequate protection of the values and the environment in which they are used.

Thus, the process of providing information security should have comprehensive basic approach that is based on a deep analysis of possible negative and positive im- pact effects [22]. Such an analysis involves mandatory identification of possible sources of threats, the factors contributing to their display (vulnerabilities) and, as a consequence, the determination of the actual threats for information security. We can represent this logical chain as following:

Source of threat -> Threat -> Vulnerability -> Implementation of Threat - > Effect (Damage).



Relying on concepts introduced above, we can construct the following detailed on- tological scheme for the issues of information security which contains the general relations between Threat, Vulnerability and Assets (named as information sources) and their subjective derivatives (figure 2).

Fig. 2. Detailed ontological scheme for the issues of computer's information security

3.1 The classification of computer security threats

Providing of security of information is impossible without systematic analysis of the relevant security threats. Basis of such analysis should be classification of threats

to certain basic features that gives to researcher (Expert in Information Security) gen- eral holistic view of the various variants of destructive influences and their impacts. The literature review proposed number classifications of security threats showing various aspects of this problem [23 - 27]. However, being designed for a

narrow range
of specific tasks, they can't be the basis of the total ordering threats and highlight their most significant attributes for later synthesis and decomposition that can be ef- fectively used in developing Knowledge Base Ontology of Expert System.

It is necessary to develop a generalized classification, which must allow considering several characteristics of threats as a subject of scientific research and later describe and show all possible types and derivatives. At the same time the classification
of the factors influencing on information security should be conducted with the fol- lowing requirements:

-sufficiency of the levels of classification factors allowing them to form a complete set;

- enough flexibility of classification, allowing expand set of classified factors and signs groups and make the necessary changes without disrupting the structure of the classification.

Under the security threat, as noted earlier, we can understand the situation, in which may be violated common services, such as integrity, confidentiality and availa- bility of information. Morphological analysis shows that we can highlight the follow- ing basic components of information security threats: the source impact on the infor- mation system, the method exposure, the impact of information objects, as well as the results (or damages).

These statements while developing for the classification can be selected as the ba- sic classification criteria for onward decomposition.

According to the standard [28], the factors affecting on information security can be classified by using their relationship of nature as objective and subjective, and by relation to the objects of information systems as internal and external. The general scheme of information security threats classification is shown in Figure 3.

The dividing of sources on subjective and objective is warranted on the basis of considerations to determine the guilt for the damage information. Dividing into inter-
nal and external sources is warranted because it can be different for the same methods of parrying threats to internal and external sources.

Moreover, both external and internal sources can be both intentional and uninten- tional.

Unintentional threats arise regardless of the will and the desire people. This type of threat is most often associated with direct natural or anthropogenic impacts on the physical elements of the information system and leads to malfunction of the system and / or physical damage (destruction) carriers, data processing and data transmission telecommunication channels.

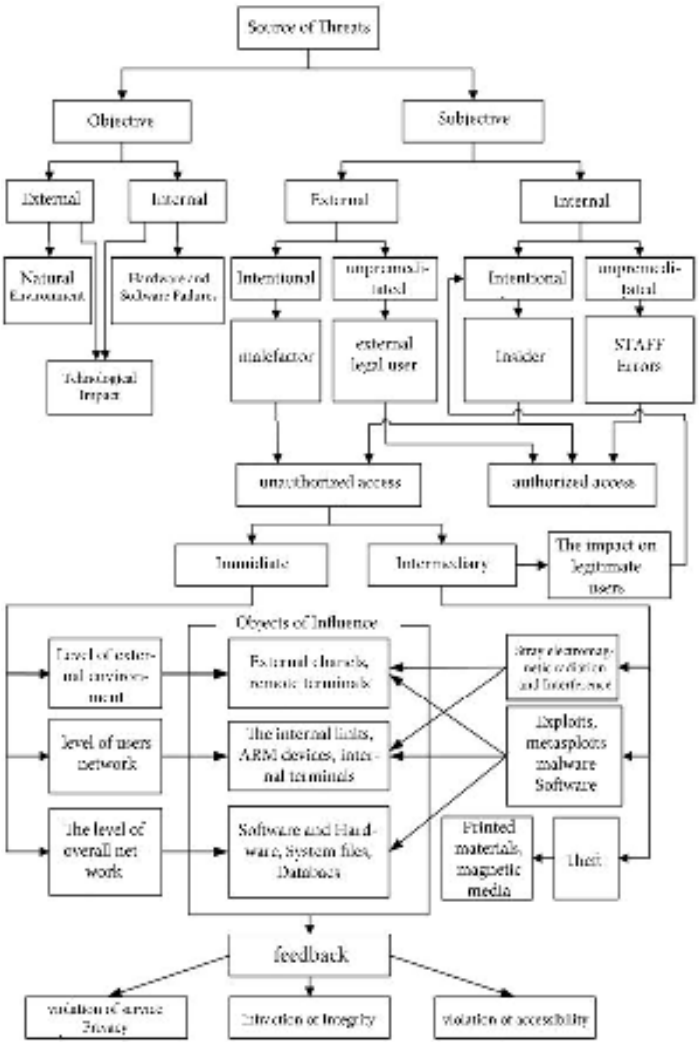


Fig. 3. The general scheme of computer and information security threats classification

Intentional threat in contrast to unintentional can be created only by people acting targeted to disrupt the work of an information system. Intentional threats may be di- vided into passive and active.

Passive threats are related to unauthorized access to information, without any amendment. Active threats associated with attempts to change (interception, modifi-

cation, destruction) of the information or attempts to disable access to the information resources of legitimate users.

Anthropogenic sources of threats

Anthropogenic sources of information security threats is the subject whose actions can be qualified as intentional or accidental violations. This group is the most exten- sive and is of most interest from the point of view of the organization of protection, as actions of the subject can be evaluated to predict and take adequate protection meas- ures. Countermeasures in this case are directly controllable and depend on the will of the organizers of information security.

As a source of anthropogenic threats we can consider subjects that have an access (authorized or unauthorized) to the work with standard means securable. Subjects (sources), whose actions may lead to a breach of information security can be both external and internal.

External actors, sources of threat, in turn, can be accidental or intentional, and may have different levels of qualifications. Below we enumerate some examples of external sources:

- criminal organizations;
- potential criminals and hackers;
- unscrupulous partners;
- technical staff telematics service providers;
- representatives of the supervisory organizations and emergency services;
- representatives of power structures.

Internal actors (sources), usually are highly qualified experts in the field of development and operation of software and hardware, are familiar with specificity of tasks, structure, basic features and principles of work software and hardware information security, and are able to use of standard equipment. For example:

- key personnel (users, programmers, designers);
- representatives of the service protection;
- support staff (cleaners, security);
- technical staff (maintenance engineering networks).

Technogenic sources of threats

The second group contains the sources of threats, determining the implica- tions technocratic human activities that can get out of it control and stand on their own. These sources of threats are less predictable directly depend on the properties of art and therefore require the special attention.

Natural sources of threats

The third group of sources of threats combines circumstances components of an ir- resistible force, that there are circumstances that have an objective and absolute na- ture, which applies to all. Overwhelming power in the legislation and contractual practices include natural disasters or other circumstances that can't be provide [29]

Natural sources of potential threats to information security are typically external to the protected object and they relate mostly to the natural disasters: fires, earth-quakes, floods, hurricanes, and various contingencies circumstances, unexplained phenomena and other force majeure circumstances.

3.2

Classification of Vulnerabilities

Vulnerability inherent in the object information, inseparable from it and are caused by deficiencies in the process of operation, properties of architecture automated sys- tems, communication protocols, and interface used by software and hardware plat- form, operating conditions and location, and etc.

Vulnerabilities may be presented in both the software and hardware, and organiza- tional and legal support to information security. The main part of the vulnerabilities of the organizational and legal support contains the lack of regulations on businesses, and issues relating to information security [30-31]. An example of the vulnerability of this type is the lack of organization in the approved concept or information security policy, which would define the requirements for Protection of Information Systems, as well as specific ways to implement them.

Vulnerabilities in software and hardware can be presented in the software or hard- ware components of user workstations, information systems servers and communica- tion equipment and communication channels for information security. Sources of threats can exploit vulnerabilities to break safety information to obtain illegal benefits (damage proprietor, owner, user information). Furthermore, there may be not mali- cious relation to sources of threats to intensify certain vulnerabilities that could be harmful.

Each threat can be compared by various vulnerabilities. Eliminating or substantially reducing the vulnerability affects is the ability to implementation of information security threats.

There are different approaches to systematizing vulnerabilities of information sys- tems and technologies. In [31], for the convenience of the vulnerability analysis they are divided into classes, groups and subgroups. Thus the information security vulne- rabilities may be divided as the following:

- objective vulnerabilities;
- subjective vulnerabilities;
- occasional vulnerabilities.

Objective vulnerabilities

Objective vulnerabilities depend on features of construction and technical characte- ristics of equipment used on the protected object. Full removal of these vulnerabilities is not possible, but they can significantly weaken the technical and engineering me- thods countering threats to the security of information. We can consider[32]:

- Related technical means of radiation (electromagnetic, electrical, sound);
- clickable vulnerabilities (hardware and software tab);

vulnerabilities determined by the characteristics of the elements (elements that have electro-acoustic transducers or exposed electromagnetic fields);

- vulnerabilities determined by the characteristics of the protected object (location object, organization communication channels).

Subjective vulnerabilities

Subjective vulnerabilities depend on the actions of employees and, in general, may be eliminated by organizational software and hardware methods. These vulnerabilities include[33]:

- Errors (during the preparation and use of the software, with management of com- plex systems, with the use of equipment);
- Violations (regime of protection and protection, the mode of operation of technical means modes of use and privacy mode, etc.).

Occasional vulnerabilities

Occasional vulnerabilities depend on the characteristics of environmental protected object environment and unforeseen circumstances. These factors are usually a little predictable, and their removal is only possible during the range of organizational and engineering activities for decreasing or mitigating threats to information security. We can consider the following types of vulnerabilities:

- Faults and failures (failures and malfunctions of technical equipment, aging and demagnetize media, software failures, failure of power supply, etc.);
- damage (lifeline
enclosing structures, etc.).
and etc.

- **Situational Sample**

Let us look at sample of security state of any university [33-36]. In the modern university a huge number of various data related not only to the educational process, but to research and engineering studies, personal information of students and staff, service, commercial and other confidential information are stored and processed con- stantly. The growth of crime in the area of high technologies dictates its own require- ments of resource protection of computer networks of educational institutions and sets
the task constructing its own integrated security system. Its solution presupposes the existence of the legal framework, the formation of the concept of security, develop- ment activities, plans and procedures for the safe work, design, implementation and

maintenance of technical equipment protection of information (EPI) within the educa- tional institution. These components define single security policy information at the university. Specificity of information security in the educational system is that the university - a public institution with a volatile audience, but also a place increased activity of "beginners cyber criminals." The main group of potential offenders is stu- dents and some of them may have a high level of training. Age range is from 18 to 23 years that contribute to youthful maximalism. The potential threats to information security may be caused by the circumstances that some young people show off in front of fellow students knowledge in arrange virus epidemic, and gain administrative access to "punish" the teacher, block access to the Internet, etc [34]. Suffice it to recall that the first computer offenses were born at the university (example is the Morris worm).

Threats to computer's information security and risk analysis of the university

For information risk analysis we should carry out the following activities:

- classify the objects to be protected, and to rank them in order of importance;
- determine the attractiveness of protection for attackers;
- identify possible threats to information security;
- consider possible ways to implement them (vulnerabilities);
- assess the damage from potential attacks on information resources.

We can distinguish the main objects of the university that are needed to protect:

- Accounting LAN data Planning and Finance Department, as well as
- statistical and historical data;
- database servers;
- Management Console user accounts;
- www / ftp server;
- LAN servers and research projects.

According to the above classification, taking into account the considered features we can study the following threats to information assets of the university (We give only some examples of threats):

Unintentional subjective Information and computer Security threats:

- TH1 - The threat of inadvertent damage to the equipment;
- TH 2 - The threat of improper shutdown of equipment;
- TH 3 - The threat of inadvertent deletion of files with important information;

Intentional subjective Information and computer Security threats:.

- TH 4 - The threat of deliberate physical destruction of the system;
- TH 5 - The threat of the scrapping of the most important components of the Infor- mation System;
- *TH 6 - The threat of shutdown subsystems provide Information System;*
- TH 7 - The threat of the scrapping of the subsystems provide Information System;

Technogenic threats:

TH8 - The threat of failure assistive technology;

- TH9 - The threat of failure of power supply system;
- TH10 - The threat of failure, the climate control system;

Vulnerability of computer systems of the university

The main vulnerabilities of cyber systems in educational institutions are:

- V1 - Having unlocked built-in accounts
- V2 - incorrectly set access rights to information resources
- V3- The presence of unused potentially dangerous services and PP
- V4 - Incorrect configuration protection
- V5 - Low level of qualification of the IS staff
- V6 - Low levels of qualifications users
- V7 - Improperly organized access to hardware IP
- V8 - incorrectly implemented concurrent access to software
- V9 - incorrectly defined user rights
- V10 - Improperly organized storage media
- V11 - Improperly organized records of media
- V12 - Missing or improperly organized system of anti-virus

Controls of Computer Security in University

Thus, the main measures and procedures of information security at the university are:

- C1 - Organization of procedures for the storage of documents
- C2 - Develop procedures for rapid response to incidents
- C3 - Administrative and technical means of monitoring the work of
- users
- C4 - Use of licensed certified
- C5 - Restriction of access to the software
- C6 - Technical support for hardware resources
- C7 - Backup
- C8 - Learn the basics of information security staff
- C9 - Corporate Culture

- C10 - Measures to prevent conflicts in the team
- C11 - The development of the internal regulatory documents for the IS

Therefore in expert system through the holding procedure of questionnaire that is described in paper [4] we define Threats (THi), Vulnerabilities (Vi) and Controls (Ci) rules of expert systems knowledge engine. The received rules are in the following:

- R1: IF V1 and V2 are LOW THEN TH5 is HIGH and C1 is LOW
- R2: IF V4 and V3 are LOW THEN TH5 and TH6 is HIGH and C2 is LOW
- R3: IF V7 is LOW THEN TH5 is HIGH and C1 is LOW
- R4: IF V4 and V6 are LOW THEN TH5 is HIGH and C1 is LOW
- R5: IF V1 and V2 are LOW THEN TH2 is HIGH
- R6: IF V11 is VERY LOW THEN TH4 is HIGH and C7 is LOW
- R7: IF V1 and V2 are LOW THEN TH6 is HIGH and C10 is VERY LOW
- R8: IF V1 and V2 are LOW THEN TH7 is HIGH and C11 is LOW

Thus, according to the rules above we a can calculate which controls are low and needed to be maintained again. This distinguished approach of ontology helps to or- ganize and define appropriate rules according to ISO standards. And according to controls we can generate recommendations for this particular situation.

Summarizing sample above we can say that:

Information resources management of higher education in current conditions is im- possible without scientific evidence and practical implementation of a balanced policy of information security [34-36].

Higher education institutions have a number of features that must be considered when building a system of information security. Specificity of information security in the educational institution is that it is - a public institution with volatile audience, as well as a place of increased activity "beginners cyber criminals."[35]. Features of the university as an object Information is also associated with a multi-character activities, the variety of forms and methods of educational work, the spatial distributed infra- structure (branches, representative offices), and so on.

• Ontology and ISO 2700K mapping

Since we are developing an expert system based on the standard of information se- curity, there is a need to find conformity between the point of standards (ISO 2700k) and of the ontology that we developed above. Let us consider the table of ontology that was prepared by using help of experts in Information Security auditing process

Based on the work, we can see that the standards are crossing in items with the ontology which is given above. Let's look at a few examples of where we can make a topology on table 2. Before we have to define vulnerability categories and threats in numbered way (see table1). It is a rough subcategory that is based on threats and vulnerabilities table.

Table 1. Identification of vulnerability and threat

Vulnerability	**ID of Vulnerability**
Subjective Vulnerability	1
Objective Vulnerability	2
Occasional Vulnerability	3
Threat	**ID of Threat**
Unintentional subjective Information Security threats	1
Intentional subjective Information Secu- rity threats	2
Technogenic threats	3
External Intentional Male Factor unau- thorized access	4
External unintentional External legal user Authorized access	5
Internal Unpremeditated Staff errors	6

Table 2. Mapping of clauses and given vulnerabilities and threats

Clause		**T h r e a t**

Security Policy		6, 2
Organization of Information security		4, 6, 5, 2
Asset Management		6, 3, 4, 2
Human Resource Security		6, 3, 2, 4
Physical and Environmental Security		6, 5, 4, 3, 2
Communications and Operations Management		5, 4, 6, 3, 1
Access control		6, 5, 4, 2, 1, 3

Business Continuity Management		6
Compliance		6

We can mention that the Internal Unpremeditated Staff Errors are common and popular threat, then External Intentional Male Factor unauthorized access threat is the second most popular factor. According to Vulnerability table Subjective Vulnerabili- ties are most common whereas Occasional Vulnerability is the second often meeting in this ISO standard.

- **Conclusion**

Summing up all the above, we can state that the task of improving the security of information systems and technologies in current conditions characterized by complex- ity, uncertainty, related to the large number of internal and external factors affecting information security. To solve the problem of information security, particularly all you need to perform the identification of assets and set the initial level of security that meets in the Information Systems. The identification process should consider the main characteristics of asset: information value, the sensitivity of the assets to the threats, the availability of protective measures. It is necessary to note that among the
factors that affect the safety, special place is occupied by the subjective factors that potentially are the most dangerous.

Ontology of knowledge base security of information systems can be described as following:

- problem area of complex security tasks
- information systems (concepts that define the essence of information security, and communication between them);
- threat to safety-critical Information Systems (external and internal objective fac- tors, external and internal subjective factors);
- measures and technologies to provide a comprehensive security of information systems;
- a comprehensive methodology for Information Systems Security (heuristic know- ledge about the state of security of information systems, strategies for integrated Security)
- identification of the assets of Information Systems, the definition of criteria and performance security, development assessment procedures of the criteria and indi- cators to develop a model integrated provision

of Information Security,etc.

- principles of integrated Information security (systemic, adaptability, transparency and confidentiality, continuity, learning and the accumulation of experience, etc.).

Thus, the solution of the problem area provides complex security (the aggregate of the basic concepts that define the essence of the study, and the links between them), including: the subject area purpose of the study, tasks, possible tactics and strategies used to achieve this goal. The analysis in this study allowed us to construct an onto- logical scheme of subject area with in-depth branches and the main criteria for the definition of such concepts as vulnerability, threat, to classify the sources of threats and vulnerabilities Security of Information Systems, to identify the characteristics of
the process of building models offender, to identify the main types of attacks on in- formation resources identify the main types of damage to information assets, to classi-
fy the methods of information and build ontological model of the information security threats. In order to achieve these purposes we proposed development of Vulnerabili- ty&Threat Security ontology mapping to ISO Standards where we find out the most common vulnerabilities and threats.

We have considered an example of the use of information security ontology in practice example to ensure the vulnerability of the university. Which were clearly shows the rules as well as the type of threats and vulnerabilities as well as Controls. Thus developed the main points of ontology information security system of an expert system in the field of information security audit

References

- Val Thiagarajan, B.E. 2002. BS 7799 Audit Checklist. Available: www.sans.org/score/checklists/ISO_17799_checklist.pdf
- ISOIEC 27002 2005 Information Security Audit Tool. Available: http://www.praxiom.com/iso-17799-audit.htm
- Stepanova, D., Parkin, S. and Moorsel, A. 2009. A knowledge Base For Justified Informa- tion Security Decision-Making. In 4th International Conference on Software and Data Technologies (ICSOFT 2009), 326–311.
- Atymtayeva L., Kanat Kozhakhmet, Gerda Bortsova, Atsushi Inoue. Methodology and On- tology of Expert System for Information Security Audit //Proceedings of the 6th Interna- tional Conference on Soft Computing and Intelligent Systems and the 13th International Symposium on Advanced

Intelligent Systems, 20-24 November 2012, Kobe, Japan , pp. 238-243

- Atymtayeva L., K. Kozhakhmet, G. Bortsova. Some Issues of Development of Intelligent System for Information Security Auditing // Proceedings of the International conference of Computational Intelligence and Intelligent Systems 2012, June 1-2, 2012, London, UK, Vol. 2, pp. 725-731.
- Atymtayeva L., K. Kozhakhmet, G. Bortsova, A. Inoue. Expert System for Security Audit Using Fuzzy Logic. // Proceedings of The 23rd midwest artificial intelligence and cogni- tive science conference, MAICS , April 21-22, 2012, Cincinnati, USA, pp. 146-151. http://ceur-ws.org/Vol-841/
- Atymtayeva L.,A. Akzhalova, K.Kozhakhmet, L. Naizabayeva. 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
- Tsudik, G. and Summers, R. 1990. AudES - an Expert System for Security Auditing. IBM Los Angeles Scientific Center.
- S. Fenz and A. Ekelhart, “Formalizing information security knowledge,” ASIACCS ’09: Proceedings of the 2009 ACM symposium on Information, computer and communications security, ACM, 2009.
- Threats catalogue on Information Systems Information technology —Security techniques — Code of practice for information security management, 2005.
- ISO/IEC. ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management, 2005.
- http://www.odbv.org
- Maljuk AA Information Security: Contemporary Issues / / Security Information tehnolo- giy. 2010. - No 1. - P.5-9.
- Domarev VV Safety of information technology. The System approach. - Kiev, Publishing house "Diasoft", 2004, 992s.