UDC 004.056

Tarasov D., Andrukhiv A.,
Information Systems and Networks Department,
Lviv Polytechnic National University,
S. Bandery Str., 12, Lviv, 79046, Ukraine

ALGORITHMS OF THE CORPORATE INFORMATION SYSTEM'S PROTECTION ANALYSES

The tasks and methods of protection corporate information systems audit are considered. The modern algorithms of estimation conducting of protection of corporate informative systems are analysed, in particular RiskWatch, CRAMM, GRIF. Considered algorithms give the possibilities to evaluate the effectiveness of protection information measures taking into consideration the information security expences towards the evident risks of information security policy violation.

1. Introduction

Nowadays a few mechanisms and standards are developed for estimation of protection information conducting. Each of the developed approaches has the features which are based on properties and descriptions of the corporate informative system objects. A basic idea during conducting of analysis is based on the system risk's analyse application, that allows to estimate the risks existing in the system and to choose the variant of optimum protection on efficiency (on correlation of risks existing in the system to the expenses on informative safety)

2. Analysis of the last researches

The standardized methods of protected information system (IS) analysis do not exist for today, that is why in concrete situations the algorithms of actions of public accountants can substantially differ. However it is possible really to build the general model of conducting of audit. A model must include the following steps [8]:

- Initiation of audit procedure. An audit is conducted not on the initiative of public accountant, but on the initiative of a company guidance, which is the most interested part in it.
- Collection of audit information. Here such information enters as organizing structure of users and attendant subsections, information about a proprietor and developer of subsections, composition and structure of the systems of protection of information, and etc
- Data analysis.Risks estimation which are related to realization of safety threats can enter here, analysis of mechanisms of organizing level safety, policy of organization safety, document, on providing the mode of informative safety and etc.
- Generation of recommendations. On this step after conducting of analysis the list of recommendations is generated on perfection (replacements) of aspects which influence general strength security of the system.
- Preparation of public accountant report. This report is the basic result of audit's conducting. It must contain the description of audit's conducting aims, description of explored IS, pointing of conducting audit border and used methods, results of data audit analysis, conclusions which are based on these results and contain estimation protected IS (PIS) level or accordance to the requirements of standards and recommendation of public accountant on liquidation of the existed drawback and perfection of the protection system.

The results of audit allow:

- to define the substantial lacks of PIS;
- to define accordance/disparity to the standards of PIS with a purpose subsequent of the system certification;
- to estimate the charges of IS proprietor in the case of threat realization and etc.

3. Estimation of protection

For electing of audit realization tools it is necessary to carry out research and comparison of descriptions of audit instruments of protected IS [9].

To basic descriptions belong: cost of license, possibility of high-quality determination and quantitative estimation, construction of the detailed report, methods of estimation and possibility of audit verification results.

The general model of audit conducting can be represented on the following scheme.

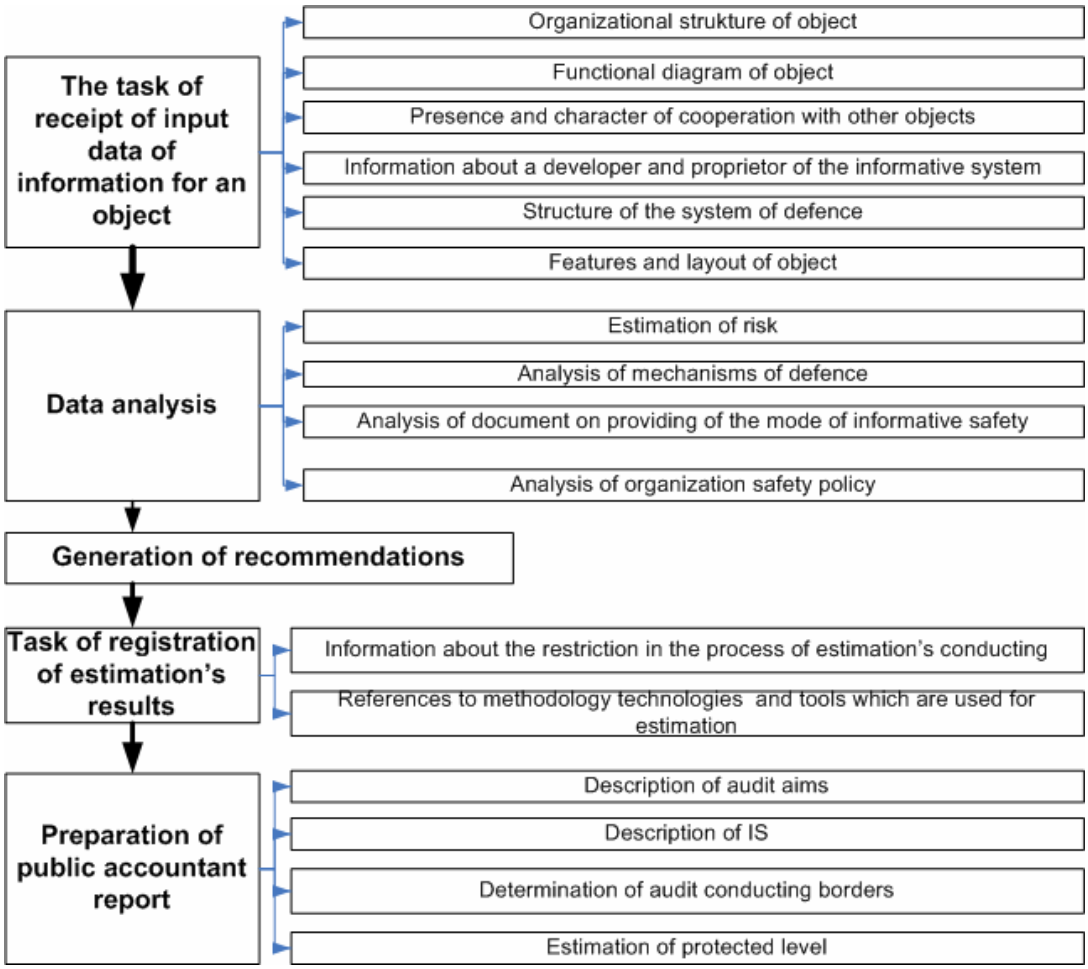

Fig.1 Basic stages of conducting protected estimation

A formula for the calculation of risk consists of three components :

- cost of resource (Asset Value, AV) . This size characterizes the value of resource.
- measure of resource's impressionability to the threat (Exposure Factor, EF) . This parameter shows in which degrees a resource is impressionable in relation to this threat.
- estimation of realization probability of threat (Annual Rate of Occurrence, ARO) shows how many credible realization of certain threat is on the certain period of time (usually, for a year).

o Estimation of the expected losses hatches on the basis of findings (risk level) [7]:

- estimation of the expected possible losses from single realization of certain threat (Single Loss Exposure, SLE) settles accounts on a formula SLE= AV*EF;
- total possible losses from the concrete threat for the year of (Annual Loss Exposure, ALE) characterize a risk size and is determined on a formula ALE= SLE*ARO

Thus the eventual formula of risk calculation assumes the view:

$$ALE= ((AV*EF=SLE)*ARO). \quad (1)$$

Risk estimation can be given taking into account both quantitative and quality measures .

As an example we will conduct the quality calculation of informative risks.

We have the server of trading company that gets busy of selling computers technique through an own Internet-shop. We will assume that annual trade turnover folds 50 thousands of dollars in a year. A server uses Microsoft IIS , Microsoft SQL Server. To make the calculation simple will adopt two models of violators : external legal user and external hacker.

First we will designate as A1, and second – A2.

There can be the identified following threats in the server relation :

- violation of information integrity ;
- violation of server availability;
- violation of information confidentiality .

The results of threats authentication and construction of violators model are represented in a table.

TABLE. 1.

Threats identily and violator model

Resource	Value of resource	Threat	Model of disturber	EF	ARO	SLE, th. $	ALE, th. $
Web-server	3	Violation of integrity	A1	3	2	9	18
		Violation of confidentiality	A1	3	2	9	18
		Violation of availability	A1, A2	2	3	6	18

In this table:

- Value of resource is determined : 1- minimum cost, 2- average cost, 3- maximal cost;
- EF (measure of resource impressionability to the threat) is determined: 1- minimum measure of impressionability (weak influencing), 2- middle (it is needed to proceed in a resource), 3- maximal (replacement of resource after threat realization);
- ARO (estimation of threat realization probability) is determined: 1-low, 2- middle, 3- high.

The resource of server is critical for functioning of company, that is why it is appropriated value AV=3. To the threat of integrity violation (EF) is appropriated maximal value (3), because violation of stored information integrity is instrumental in derangement of supplies. Probability of threat realization of integrity violation is appraised as middle. Parameters of EF and ARO in the relation of threats violation of confidentiality and availability are settled in the same way. Most parameters, except for AV was founded from expert opinion of public accountant.

All identified risks are high, as realization of these threats, will inflict substantial harm to the company.

A company must use measures on the decline of risk value. In this case such measures can be server tuning, establishment of net-to-net relay screen software.

We will count expenses on introduction of the indicated measures. For example, tuning of server software will bear in 20 man-hours, and the financial investments will take 1000$. Establishment of net-to-net relay screen: 50 man-hours and 5000$. Thus, general expenses on introduction of the offered measures – 70 man-hours and 6000$. In comparison with the annual turn of Internet-shop these expenses though high, but are fully justified. The most important, that the risks should be correctly identified and ranking in accordance with the degree of their organization criticism .

Now in the world market represented 3 base algorithms are represented for the calculations of risk: GRIF, CRAMM, RiskWatch.

4. RISKWATCH

In the method of RiskWatch as criteria the “possible annual losses” (Annual Loss Expectancy) and estimation of “returning are elected from investments” (Return Investment). Algorithm of RiskWatch in general case is possible to be taken to the following steps:

1. Determination of the research article . Here is determined the type of organization , base requirements in the regions of safety, composition of organization.
2. Data which describe concrete descriptions entry. On this stage resources, losses, classes of incidents, are described in detail. Frequency of each making is set of possible threats, degree of impressionability and value of resources.
3. Determination of risk. At first a connection is established between resources, losses, threats, vulnerability.A mathematical hope for the risk for a year settles accounts after a formula:

$$R=p*D, \quad (2)$$

where R – is value of risk; p – frequency of threat in a year; D – is the cost of resource.

4. Generation of report. It can be the report of losses from realization of threats; report about measures on counteractions; report about the result of safety audit and etc

Software realized on the basis of method has such drawbacks :

- the analysis passes at programmatic-technical level of defence and administratively-organizational factors are not taken into account;
- absence of complex approach to informative safety.
- high cost of license.

5. CRAMM

Method CRAMM is more powerful and more universal instrument. A method which connects the quantitative and quality analyses methods and it presents complex approach to estimation of risks.

Method CRAMM foresees the presence of such stages of analysis:

- on the first stage present strength security of resources is determined. If this level is low, to the system the minimum set of requirements of safety is produced and transition is carried out on 3 stages.
- on the second stage authentication of risks is conducted and their size is determined. A public accountant collects basic data from the representatives of organization.
- management by the risks, choice of counter-measures. In this case the ground of the chosen counter-measures is a major criterion.

It is possible to represent the conceptual chart of CRAMM

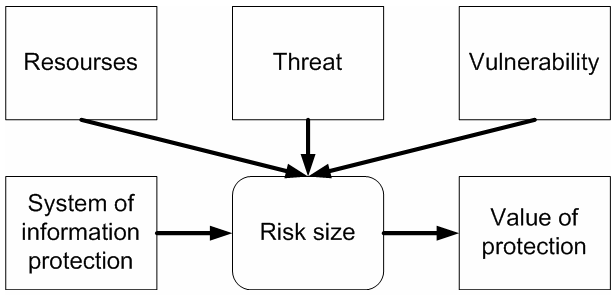

Fig. 2 Conceptual charts of method CRAMM

To the strong side of method belongs:

- well structed and tested method;
- in basis of software product there is a good knowledges base on counter-measures in the field of informative safety;
- flexibility and universality of method allows to use it for the audit of IS arbitrary level of complication and purpose;
- it is possible to use as tool of documenting present mechanisms of IS safety .
- The lacks of the method:
- requires the special preparation and high qualification of public accountant;
- audit according to this method is very complex and requires a lot of time;
- there is no possibility to change the template of reports;
- high cost of license.

Above mentioned the resulted algorithms take approach, when an user specifies the complete list of safety threats , that specific for this system together with estimation of losses on every type of threats. However the fact is not taken into account , that to one type of information can be directed at once a few threats, that in the turn will result in that total losses are calculated to the threats will be unrealistic. Taking into account this fact, that information is the object of protection, the algorithm of risk analysis must push off not from the threats and losses on by it, but from information and from losses on information, but here to take into account threats.

6. Algorithm GRIF

Comparatively with other algorithms, GRIF has a row of substantial advantages allows to disengage oneself on the stage of design of the system from the threats of safety, an algorithm allows to break up IS on the certain great number of situations, where the analysis can be conducted on each of these parts. Taking into account practical and easy usage it is suggested to consider this algorithm in details [4].

Algorithm foresee two office hours – when one base threat is considered and when three base threats are. In this review we will consider one base threat. During work with an algorithm a scale is used from 0 to 100%. A scale can be broken up on 100 parts. Every part occupies a certain interval. Laying out can be conducted evenly and logarithmic. For example, for 5 levels the even laying out will look like this: 1 level – 20%, 2 levels – 40%, 3 levels – 60%, 4 levels – 80%, 5 level – 100%; logarithmic – 1 level – 7%, 2 levels – 18%, 3 levels – 35%, 4 levels – 62%, 5 level – 100%.

1. On the first stage of work of algorithm of threat level calculation is conducted on impressionability of Th on the basis of criticism and probability of threat realization through this impressionability. The level of threat provides for as far as critical there is influence of this threat on a resource taking into account probability of its realization.

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}, \quad (3)$$

where ER – is criticism of threat realization (it is specified in %), P(V) is probability of threat realization through this impressionability (it is specified in %), Th – is the level of threat on impressionability.

2. The second stage foresees the calculation of threats level on all vulnerability CTh, through which is possible the realization of this threat on a resource. Let's sum up the levels of threats through impressionability after the following chart:

$$CTh = 1 - \prod_{i=1}^{n} (1 - Th_i), \quad (4)$$

where CTh – is the level of threat on all vulnerability, Th – is the level of threat on impressionability.

The value of threat level on all vulnerabilitie must be in scopes from 0 to1.

3. On a third stage like we expect the general level of threats on the resource of CThR (taking into account all threats which influence on a resource)

$$CThR = 1 - \prod_{i=1}^{n} (1 - CTh_i), \quad (5)$$

where CThR – is general threats level on a resource, CTh – is level of threat on all vulnerability.

The value of general level of threat must lie in an interval from 0 to 1.

4. On the resource of R is expected following risk:

$$R = CTh \times D, \quad (6)$$

where R – is risk on a resource, CThR – is general level of threats on a resource, D – is criticism of resource.

Criticism of resource is determined according to the next formula.

$$D = D_t \times T, \quad (7)$$

where D_t -- is criticism of resource on the threat availability in an hour, T – is maximally critical time of resource outage.

5. The risk on IS – CR reckons with a formula:

In money :

$$CR = \sum_{i=1}^{n} R_i, \quad (8)$$

where CR – is risk on IS, R – is resource risk.

In levels:

$$CR = (1 - \prod_{i=1}^{n} (1 - \frac{R_i}{100})) \times 100, \quad (9)$$

where CR – is risk on IS, R – is risk on a resource.

The analysis of informative risks is a difficult practical problem. Approaches to its realization can be most different – from simple enough, but comfortable and powerful (RiskWatch) to the systems very difficult in work (CRAMM). RiskWatch and CRAMM operates with the concrete types of threats and line up the difficult model of IS[6]. Method GRIF is based on the complex parameters which are determined by protected explored object. It is analysed as technological aspects of protected question of complex safety.

The comparative analysis over of methods can be brought to the next table [5].

TABLE 2.

The comparative methods analysis

	CRAMM	RiskWatch	GRIF
Supporting	Present	Present	Present
Type of estimation	Quality	Quantitative	Quantitative + Quality
Simplicity in the use	Special preparation	Special preparation	Does not need the special preparation
Price for software	2 000$ – 5 000$	More then 10 000$	More then 1 000$

7. Conclusions

The use of the resulted methods is divided geographically, namely – RiskWatch is used on the territory of the USA, CRAMM in Great Britain, GRIF – in CIS [1]. Among the resulted methods GRIF owns the best descriptions – comparative low cost licenses, possibility of determination of quality and quantitative estimation, construction of the detailed report, the use of programming systems on the basis of this method does not need special knowledge.

Conducting of risk estimation does not allow to argue investments, as it is impossible to define exact numbers (and during conducting of quality analysis they disengage oneself) for determination of expenses on diminishing of risks. For the ground of charges it is needed to identify measures which will allow to decrease the risks to the acceptable size. Measures on the decline of risks, as a rule are always concrete (technically or organizationally). And it is in this case already possible to talk about a cost. Estimation of necessary measures in a money equivalent is conducted after acceptance of budget [3]. Thus determination of risk estimation can serve as basis for bringing in of investments.

References

[1] Guide for Production of Protection Profiles and Security Targets. ISO/JTC1/SC27/N2449. DRAFT v0.9, January 2000.

[2] Information technology – Security techniques – Protection Profile registration procedures. ISO/IEC 15292 : 2000 http://www.iso.ch/iso/en/commcentre/pdf/Itsecurity0006.pdf

[3] *Астахов А.* Основные классы угроз в компьютерном сообществе, их причины и способы устранения. http://jetinfo.isib.ru/2004/2004.16.pdf

[4] *Куканова Н.*, Методика оценки риска ГРИФ 2006 из состава Digital Security Office http://www.dsec.ru/about/articles/grif_ar_methods/

[5] *Куканова Н.*, Современные методы и средства анализа и управление рисками информационных систем компаний http://www.dsec.ru/about/articles/ar_compare/

[6]*Липаев В.В.* Анализ и сокращение рисков проектов программных средств http://jetinfo.isib.ru/2005/1/2005.1.pdf

[7] *Сидак А., Марк К.* Методология оценки безопасности информационных технологий по общим критериям, http://jetinfo.isib.ru/2004/6/2004.6.pdf

[8]С*имонов С.*, - Технологии и инструментарий для управления рисками http://jetinfo.isib.ru/2003/2/2003.2.pdf [6]

[9] Тарасов Д.О. Аудит баз даних// Защита информации: Сборник научных трудов. – Киев: КМУГА, 2000. с.137-143.