Nonlinear Phenomena in Complex Systems, vol. **17**, no. 3 (2014), pp. 296 - 300

Approach to Assessment of Measures Sufficiency of Confidential Information Protection

A. F. Suprun
Saint-Petersburg State Polytechnic University,
29 Politechnicheskaya Str, 195251 Saint-Petersburg, RUSSIA
(Received 27 March, 2014)

Algorithm to create an end-to-end system of monitoring the security of potential information leakage channels with reference to structures, engaged in handling confidential information has been proposed. The technology for constructing a model of estimating sufficiency of protection measures, including a technique to detect threats to confidential information has been offered. Technique to rank technical channels of information leakage has been presented.

PACS numbers: 89.70.-a
Keywords: information security, monitoring system

1. Introduction

Complex protection is a set of organizational, technical and special technical activities aimed at prevention of information leakage during processing confidential information [3].

It is known that any protection is targeted at preventing and reducing damage. However, when it comes to the National Security Information, damage reduction is not only a single target, it protects national security. Therefore the main purpose of the complex protection is "to meet the targets with the minimum loss of confidential information":

$$\prod = \min\{\prod_i\}$$

where $\prod_i$ is a number of leakage channels of i-type with limited protection resources and lack of time.

Such a definition emphasizes a subordinate role of protection as one of the supporting subsystems which contributes to successful performance of information processing structures.

The main goal of the complex protection is achieved via solution of the fundamental task - preservation of confidential information at technological storage, processing and transmission.

Organization and implementation of the complex protection are based on four underlying principles: complexity, continuity, operativeness and sufficiency [1].

Complexity implies protection at all stages of information processing: from input to destruction. The information processing cycle consists of the following stages: input, transmission, retrieval, usage, dissemination, destruction.

Protection **continuity** implies a constant and uninterrupted succession of protective measures, i.e. at all stages of information processing. Formally, under threat to confidentiality, this principle of information processing is presented as an operating model, which is a sequence of actions to achieve a functional goal. Every stage has to be completed with the probable preservation of confidentiality,

$$P_c(\tau_\phi) = \prod_i P_c(t_i)$$

where $\tau_\phi = \sum_i t_i$ is a run period; t_i is a period of the i-th stage; $P_c(t_i)$ is a probability of confidentiality preservation at the i-th stage.

The **operativeness** principle requires timely protective activities and readiness for implementing the targets.

The principle of **sufficiency** implies that an amount of protective efforts should guarantee appropriate security of information processing.

The structure of the complex protection is comprised of two functionally independent protective barriers: active and passive protection.

Security in this case is described by the expression:

$$P_{c3}(T) = 1 - [(1 - P_{c3}^{a}) \cdot (1 - P_{c3}^{n}(T))]$$

where P_{c3}^{a}, P_{c3}^{n} is a probability of security preservation provided by active or passive protection respectively.

According to the conceptual models of complex protection, confidentiality of information processing is provided by organizational, technical, software/ hardware protective measures [3]. Sufficiency of the complex protective measures is estimated by the end-to-end monitoring system (EMS) introduced in the institution.

2. Algorithm of creating the end-to-end Monitoring System

End-to-end monitoring systems are expected to control sufficiency of protective measures aimed at security of information processing.

EMSs are developed by information security structures or people in charge of this field in cooperation with developers and maintainers of information objects. Besides, EMSs can be created with the involvement of chartered contactors and outsourcers.

EMSs creation is divided into three stages:

1. pre-design stage, which includes a list of protected technical channels, control techniques and funding resources;

2. EMSs development stage;

3. stage of EMS launch, which includes purchase, installation, operational testing, acceptance testing.

Having analyzed different approaches to solving these tasks, we come up with the following algorithm to develop EMSs (fig. 1).

The prerequisite for the EMS development is a level of protection requirements determined by a security class of an information object [5].

According to Russia's Federal Service for Technical and Export Control, a security class predetermines a number of primary information security techniques, ignoring additional ones.

The additional techniques allow for specific features of information processing and a number of other factors, including financial resources of an organization [2].

The sequence and content of further steps and relevant factors of information security are presented in the figure above.

3. Methods of detecting threats to confidential information

The policy of information security in the area of minimizing risks and smoothing consequences of different threats to confidentiality requires following rational proportions in budgeting. Obviously, a ratio of the budgeted funds for security shall be in line with not only a number of possible leakage channels, but the extent of every threat [4]

In order to compare estimates, it is necessary to apply the aggregate threat indicator. As the aggregate threat indicator we can use a linear set of indicators which characterize the channels by different threat parameters:

$$Y = \sum_{k} \beta_k Y_k, \quad k = 1, \ \ldots, \ m$$

where Y_k is a k-threat indicator;
β_k is a weighting coefficient ($\sum_k \beta_k = 1$).

The quantitative estimate of a threat qualitative property can be obtained through comparing channels with each other. The obtained estimates are relative, as they depend on what leakage channels are compared to. Relative threat weights with the small number ($m \leqslant 10$)

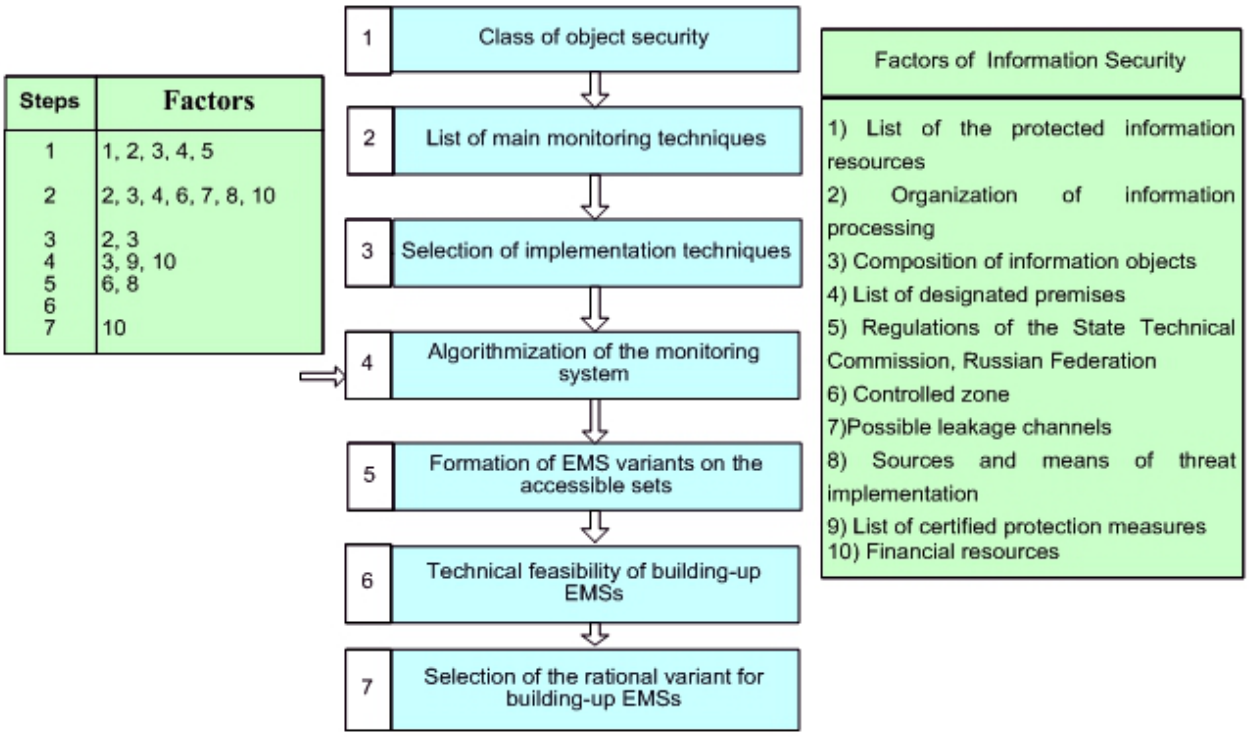

FIG. 1: Algorithm of EMS development.

can be stated intuitively – the expert relies on his/her professional competence. If the number is large ($m>$ 10), relative weights are estimated by a formalized procedure.

For the relative estimate it is necessary to define a fuzzy variable, which describes the channel threat, and build up the membership function for the fuzzy sets' content, formalized by the fuzzy variable.

In order to obtain the quantitative estimates of the integral threat, we will enter a fuzzy variable "channel under threat expressed on the discrete set $\Theta = \{\theta\}$ out of m channels. The fuzzy set $\tilde{A}$ on the sets Θ represents the aggregate $\tilde{A} = \{< \mu_A(\theta)/\theta >\}$ where $\mu_A(\theta)$ is the membership of the channel $\theta \in \Theta$ to the sets $\tilde{A}$. This can be explained as a subjective probability. High values $\mu_A(\theta)$ correspond to the channels which conform to the selected fuzzy variable.

In order to calculate the channel membership to the fuzzy set $\tilde{A}$, we will use the method of pair comparisons by a qualitative property with a preferred quantitative estimate. Matrices of the pair comparisons are obtained on the basis of the expert poll referring to how much the channel θ_i conforms to the content of the fuzzy variable "channel under threat" compared to the channel θ_j. The expert makes estimates w_{ij} using the T. Saaty rating scale (table 1) and compares the expected channel threats.

In order to enhance validity of the calculated relative weights, we applied the following techniques:

1) a group of z experts is invited for assessment to diminish subjectivity of estimates. Hereby relative weights of channels for a particular property represent every group member's averaged weights or the ones which result from experts' competence;

2) experts' agreement is estimated to check practicality of the obtained results. Hence it is

Table 1: Expert estimation of threat levels

Estimates W_{ij}	Definition	Explanation
1	Channels are equally threatened (unthreatened)	Channels are similarly dangerous
2	Intermediate value	
3	Slight advantage	Expert believes that the threat to the first pair channel is slightly higher than the second one
4	Intermediate value	
5	Big advantage	Expert believes that the threat to the first pair channel is unquestion higher than the second one, which confirms the statistics
6	Intermediate value	
7	Decided advantage	Expert has no doubts that the threat to the first pair channel is unquestionable higher than the second one, which confirms the statistics
8	Intermediate value	
9	Absolute advantage	Expert has no doubts that the threat to the first pair channel is considerable higher than the second one

necessary to calculate variation coefficients:

$$\vartheta_{ij} = \frac{\sqrt{\frac{1}{z-1}\sum_{l=1}^{z}\left(w_{ij}\left(l\right) - w_{ij}\right)^2}}{w_{ij}} \qquad (1)$$

where $w_{ij}(l)$ are elements of the matrix $W(l)$, obtained from the l-th of z experts; w_{ij} is an average of the elements.

Experts' agreement is considered to be satisfactory if $\vartheta_{ij} \leq 0,3 \ \forall \ i,j$ and good if $\vartheta_{ij} \leq 0,2 \ \forall \ i,j$. If the agreement is unsatisfactory, experts have to scrutinize the results of comparisons and make corrections. After that newly filled-in matrices are processed and agreement is estimated again.

As a result of expert assessment we obtained z matrices of pair comparisons, which are not generally transitive.

After processing the matrices of pair comparisons, weights, resulted from the expert assessment, represent components of the maximum eigenvector of the pair comparison matrix W, obtained by approximate calculations. Results of comparative threat assessment of channels, presented in the form of a diagram in fig. 2, are used in the selection of IT protection.

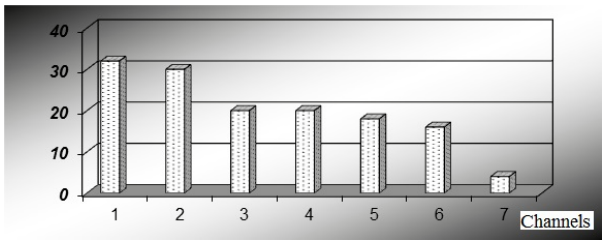

FIG. 2. Results of rating information leakage channels.

4. Conclusion

The task of estimating sufficiency of measures on complex protection of confidential information is solved via:

1. Updating data bases for possible threats and IT protection;
2. Revision of real threats to security of information objects;
3. Enhancing models and methods to solve the task of selecting a rational variant to build up the complex protection of information allowing for indicators of technical and economic efficiency;
4. Localization and life reduction of threats, specification of their processing;
5. More profound studying the security of designated premises and IT connection.

The presented methodology can be used to develop the system of complex protection for any state and municipal managerial, commercial structures which handle analytical network, system administration and confidential data base.

References

[1] P.D. Zegzhda, A.M. Ivashko. *How to build up protected information system.* (Mir i semya–95, Interline, Saint-Petersburg, 1998).

[2] E.A. Karpov, I.V. Kotenko, M.M. Kotukhov *et al. Legal, organizational, and technical support of information security in automation systems and computer networks.* Ed. I.V. Kotenko. (VUS, Saint-Petersburg, 2000).

[3] S.S. Kort. *Theoretical fundamentals of information protection.* (Helios ARV, 2004).

[4] Y.N. Nikolayev. *Design of protected information technologies.* (SPbSTU, Saint-Petersburg, 1997).

[5] A.A. Khorev. *IT protection.* Volume 1. (NPTZ "Analitica 2008).