

Managing the Process of Protection Level Assessment of the Complex Organization and Technical Industrial Enterprises

A P Gorlov¹, V I Averchenkov², M Yu Rytov¹ and V T Eryomenko³

¹ Department of Information Security Systems, Bryansk state technical university, Bryansk, Russia

² Department of Computer Technologies and Systems, Bryansk state technical university, Bryansk, Russia

³ Department of Electronics, Computing and Information Security, Priokskiy State University, Oryol, Russia

Abstract. The article is concerned with mathematical simulation of protection level assessment of complex organizational and technical systems of industrial enterprises by creating automated system, which main functions are: information security (IS) audit, forming of the enterprise threats model, recommendations concerning creation of the information protection system, a set of organizational-administrative documentation.

1. Introduction

At present, the problem of the confidential information protection is especially important. The damage from destroying, stealing, and disclosure of confidential information exceeds millions of rubles.

According to the statistics for 2014, around 120 thousand crimes associated with informational security were documented on the territory of the Russian Federation (RF). These crimes include unauthorized access to confidential information, disclosure of data constituting a trade secret, creation, use and distribution of the malicious software for computers or gadgets with such software. [1,2,3]

An industrial enterprise is an asset complex, used for the entrepreneurship activity. An industrial enterprise includes all types of property designated for its activity.

Industrial enterprises as informational objects (IO) are a complex of informational resources, measures and information processing systems used in accordance with the specified informational technology and their utilities, buildings and facilities, where these utilities are installed, or buildings and facilities designed for confidential negotiations.

If informational objects are not equipped with the Information Protection System (IPS), the confidential information can be disclosed. Design and implementation of such systems is quite expensive procedure. Generally, information processing system is influenced by a set of factors, which can be relatively divided into two categories: regulatory and legislation requirements, different threats of informational security (IS) Automated System (AS) of protection level assessment of the complex organizational and technical systems enables to provide Information Processing System correspondence to the specified requirements, prevent actual threats, decrease work labor input, save time and significantly reduce material expenditures for audit and IPS development.[4,5]

Thus, the development of assessment automated system for the protection layer of informational object is important. At the moment, automated assessment of informational security level is provided

only by ISO standards, however organizational-administrative documentation is more popular in the RF.

2. The Description of the Automated System of Informational Security Level Assessment

The proposed methods are based on the assessment of informational object protection according to the provisions of legislation base of the RF, state standards requirements, and inspection of availability of organizational-administrative documentation, which regulates the protected processing of confidential information.

The basic task of the developed AS is vulnerabilities identification of the existing systems of information processing and protection. Initial data are presented by the data about informational object, which are based on specific questionnaires.

AS Work Algorithm (Figure 1):

- Initial data enter
- Formation of informational model of informational object
- IO protection condition assessment
- Formation of IS threats model
- Formation of the recommendations concerning improvements of Information Protection System
- Formation of organizational-administrative documentation.

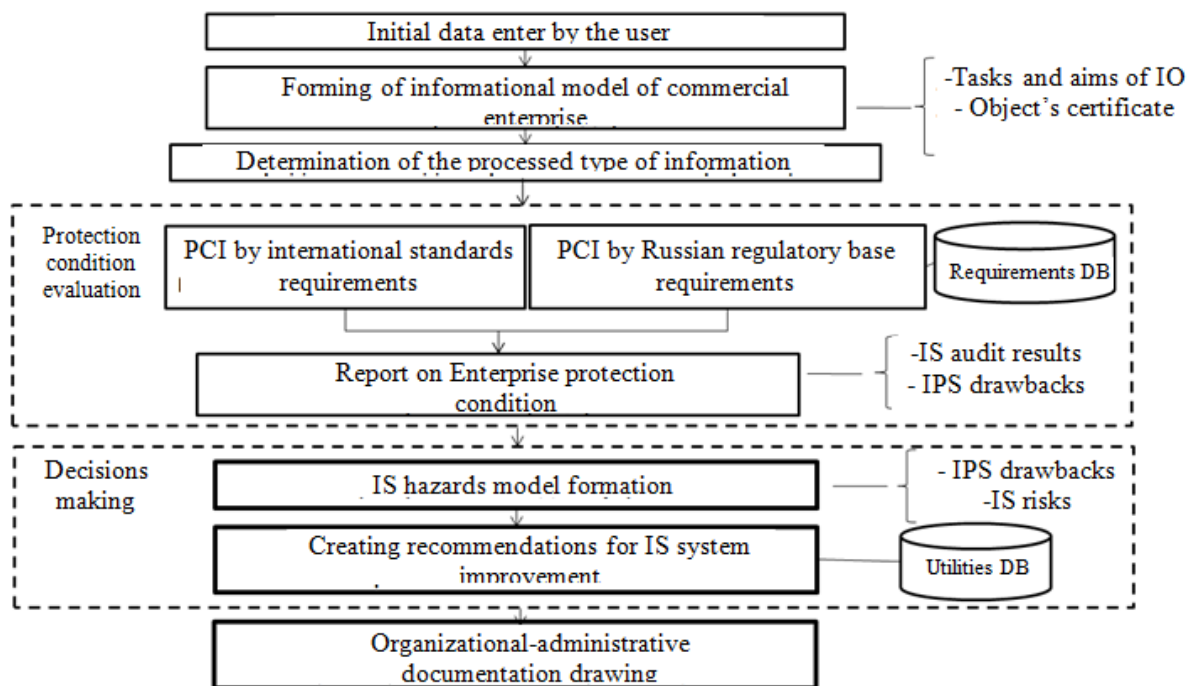


Figure 1. An AS Operation Mechanism.

The advantage of this method is the possibility to reduce work labor input, reduce temporary and material expenditures for the assessment of information security level, the increase of the design solutions quality.

The most popular is the practice of the formation of the single protection system from different elements, when already existing informational media is complimented with information protection measures. Modern conditions demand another approach which presupposes initial design of informational media concerning all of its components. This ensures the possibility to assess the practicability of any IPS at a design stage, and stimulate the IPS cooperation in the single informational space. [4]

The content and operability of the designed IPS should comply with the threats actual for the considered informational system. To comply with this requirement, the existing vulnerabilities and threats of the informational security, the degree of their importance and their implementation possibility, as well as potential threat from their implementation, should be identified at the design stage. This IPS design stage is one of the most important and labor-intensive, as the results of information security threats identification influence on the selection of measures for confidential information protection.

Automation of this process should be based on the mathematical model of vulnerabilities identification of the information protection system. [6, 7]

In figure 1, this process is presented by the protection condition assessment block.

Initial data entering is presented by the questionnaires filling, which enables to identify the type of the processed information, existing protection measures, IS threats, information protection system vulnerability, and other data necessary for the formation of the informational object model.

IO protection condition assessment is the next stage. There are 3 main divisions of protection assessment:

- Assessment of the conformance to standards requirements (GOST, STR-K, ISO)
- Identification of information technical protection measures on the informational object.
- Identification of organizational-administrative documentation, which regulates the protected processing of confidential information.

Basing on the results of this stage, the report about the condition of informational object protection is drawn.

At the stage of formation of informational security threats models, the information processing system description is formed, the system users are identified, the initial protection level is determined, and threats importance level and threats implementation level is calculated.

Risks importance is identified basing on the type of the processed information, the volume of the data processed in the system, informational structure system, data processing mode and etc.

To determine importance of the informational object threats, it is practicable to specify the importance criteria for the particular threat. Thus, for the network attack threat, the following importance criteria can be specified: access to the worldwide web, availability of firewalling and antivirus protection utilities in the local net structure.

Formation of the recommendations concerning improvements of Information Protection System is the next stage. Recommendations are divided in 3 next sections:

- Recommendations on organizational protection of information.
- Recommendations on engineering and technical protection of information.
- Recommendations on hardware and software protection of information.

A set of measures which performance is mandatory for the protection of the determined threats is provided for each section. At this stage, optimal means of technical and software and hardware information protection are selected due to the acceptable cost and a set of the required characteristics.

The final stage is drawing of organizational-administrative documentation, which regulates the protected processing of confidential information.

At this stage, organizational-administrative documentation availability on the informational object is inspected, missing documents are identified and, if applicable, the data required for the additional documentation are collected. [8,9]

Output data of this block is a set of organizational-administrative documentation, which regulates the protected processing of confidential information.

The results of the automated system operation are provided in figure 2.

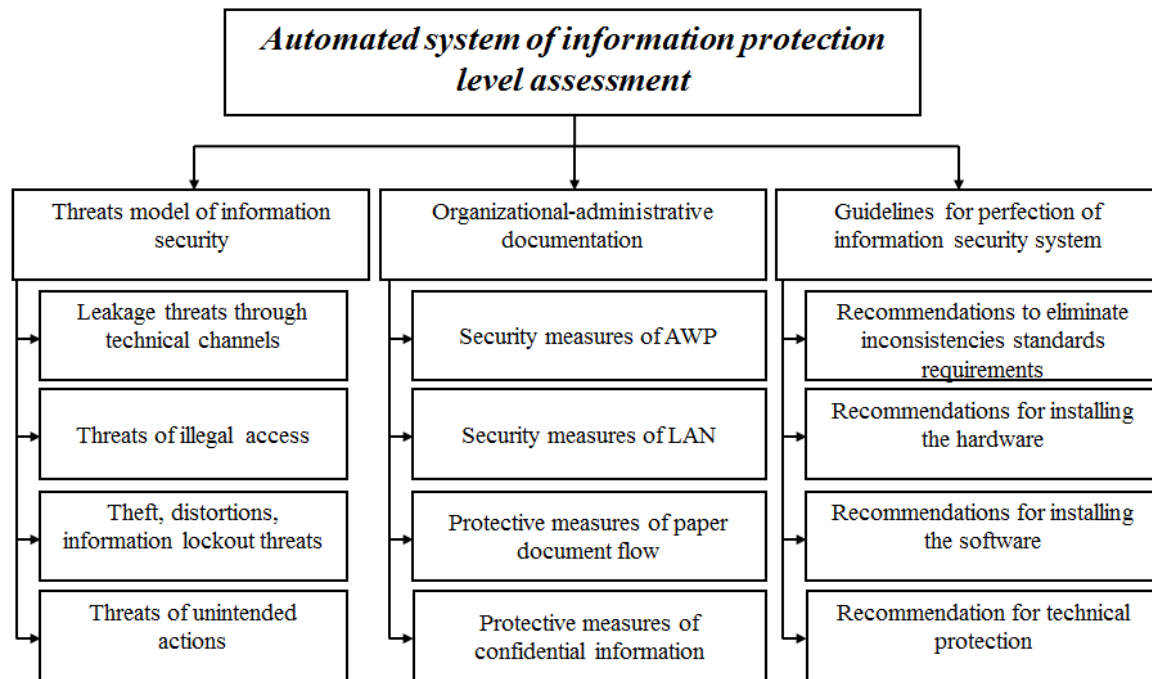


Figure 2. AS Work Results.

Thus, at the automated system output, the set of the documents including the threats model for informational security of the object, a set of organizational-administrative documentation, which regulates the protected processing of confidential information and the recommendations for improvement of information protection system, are formed.

3. Mathematical Simulation of Information Protection System Operation

The behavior of the complex informational systems, being destructively influenced from the inside and the outside, is a non-homogeneous stochastic process. In order to achieve information concerning the dynamics of multivariate problem, there should be determined the criteria in accordance with which the mathematic simulation tool will be selected (Table 1).

Table 1. Requirements to the Mathematical Model

№	Requirements to Mathematical Model
1	Possibility to account the probability of threats implementation and prevention
2	Possibility to stimulate protection processes in time.
3	Possibility of simultaneous simulation of threats implementation and prevention in time
4	Possibility to account timeliness of the safety threats protection and reaction means.

The analysis of these criteria showed that the most suitable for information protection models simulation tool is a mathematical apparatus of colored, scholastic, inhibitory Petri nets [8,10].

Colored nets enable the division of safety threats and reaction methods.

Scholastic nets enable setting of the probability of transfers (threats arising and reaction methods).

Inhibitory nets enable implementation of the threats prevention process by the reaction method.

The formal definition of mathematical model, based on inhibitory, scholastic and colored Petri nets is suggested: $F = \langle P, T, I, O \rangle$, where $P = \{p_1, p_2, p_3, p_4, p_5, p_5'\}$: p_1 – threat source, p_2 – security

threat source, p_3 – **threat** pass through vulnerable section, p_4 – reaction method forming, p_5 – destructive performance, p_5' – safety threat prevention, $T = \{t_1, t_2, t_3\}$ – set of transitions, I – initial positions, O – output positions. For timeliness simulation of the reaction of **threats** protection means the net's tokens are defined on the set $Color = \{red, blue\}$, with this in view, tokens $Color = red$ are associated with safety threats, and tokens $Color = blue$ – with the reaction methods. With this in view, positions $\{p_1, p_2, p_3, p_5\}$ can be acquired only by tokens $Color = red$, $\{p_4, p_5'\}$ – only tokens of the $Color = blue$ type.

For the formalized model of each of the transitions actuation methods $T = \{t_1, t_2, t_3, t_3'\}$, the following additional operands and parameters should be introduced:

$F(p_i)$ – function reflecting token presence in position p_i ;

$\phi(P)$ – function reflecting implementation/reflection of the threats with probability P ;

P_{threat} – attack probability;

$P_{reaction}$ – probability of threat eliminating;

Action rules are assigned with the terminal language [6] of Petri's nets:

$P1_i \rightarrow \tau_i = t1_i(FP1_i), t2_i(FP2_i, \phi(P_{threat(n)})), t3_i(FP3_i, \phi(P_{reaction(m)}), t3'_i(FP3_i, \phi(P_{reaction(m)})) \rightarrow P5_i, P5'_i$;

Petri nets fragment (colored, inhibitory, scholastic), used for IPS and threats vulnerabilities identification, is presented in figure 3:

- 1) scholastic net enables accounting both attack means and safety threats preventive means due to the adjustment of transition probabilities.
- 2) colored Petri net enables identification of the tokens, associated with safety threats and reaction methods;
- 3) inhibitory Petri net ensures implementation of a safety threats prevention mechanism by the reaction methods.

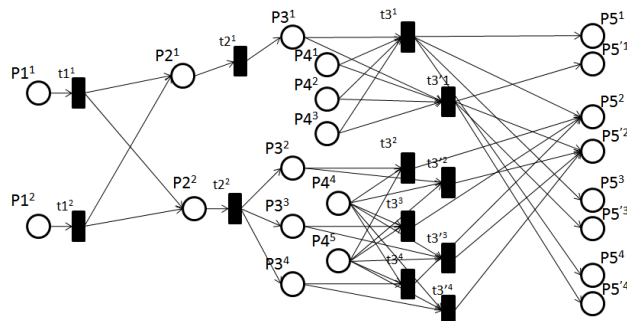


Figure 3. APetri net fragment.

Thus, the appliance of inhibitory, scholastic and colored Petri nets enables evaluation of the objects protection condition and takes into account simultaneous attacks and protective mechanisms reaction timeliness.

4. Conclusion

The suggested approach to evaluation of the informational object's protection condition enables a significant reduction of material and time expenses for the informational security audit, as well as an increase in the quality of design solution during the creation and implementation of information protection complex systems.

The mathematical apparatus of colored, scholastic, inhibitory Petri nets enables evaluation of the efficiency of the object protection system, including reaction timeliness of reaction means and simultaneous threats implementation.

References

- [1] Ritov M Yu and Gorlov A P 2014 *Information and Security* **2** 98-102
- [2] Ritov M Yu and Gorlov A P 2015 *Information and Security* **1** 108-112
- [3] Averchenkov V I, Ritov M Yu, Kondrashin G V and Rudanovsky M V 2008 *Audit of information security of state and municipal management system* (Bryansk) p 126
- [4] Hopcroft J, Motvani R and Ullman J 2002 *Introduction to Automata Theory, Languages and computing* Williams (per edition Addison Wesley) p 528
- [5] Peterson J 1984 *The theory of Petri nets and modeling systems* (Moscow) p 264
- [6] Pentus A E and Pentus M R 2006 *Mathematical theory of formal languages* (Bean. Knowledge Laboratory) 248
- [7] EUROPEAN STANDARD EN 50132-2-1 July 1997
- [8] Wei T H 1952 *The algebraic foundations of ranking theory Theses* (Cambridge)
- [9] Saaty Thomas L 1990 Eur J Oper. res **48(1)** 156-160
- [10] Cogger K O and Yu P L 1985 *J Optimiz Theory and Appl* **46(4)** 483-491
- [11] Josef Studler 1975 *Econ Math Obs* **21(2)** 185-195