Development of methods and models of computer-aided design of security system against information threats for aviation-instrument-making

V E Trushnikov¹, N N Baranova², M V Grishin³

¹Doctor of Technical Sciences, Professor, Professor of the Department of System Analysis and Management, St. Petersburg Mining University, St. Petersburg.
²Designing engineer of Ulyanovsk Instrument Design Bureau JSC, Ulyanovsk
³Grishin Maxim, Ph.D., Designing engineer of Ulyanovsk Instrument Design Bureau JSC

E-mail: Trushnikov_VT@pers.spmi.ru

Abstract. The article discusses the problems of existing methods of computer-aided design for protecting confidential information of design enterprises of the tool manufacturing industry. The method is described on the basis of a modular, unified approach to security systems. A simulation model of information security threats was developed for the instrument design engineering bureau.

1. Introduction

In the context of information threats to manufacturing enterprises, there is no single method for the automated design of information protection systems.

The heterogeneity of information systems used at instrument-manufacturing enterprises does not allow for the end-to-end interaction of co-executing enterprises and customer organizations, which makes it difficult to implement infrastructure solutions [1]. There is a lag in the level of development of Russian standards on information protection, including national standards [2] for describing the digital architecture of enterprises. There are no process management methods, legal support for the use of electronic design, technological and operational documentation as part of the life cycle of defense products.

Almost all organizations use foreign computer equipment and system-wide software. This entails the technological dependence of most industries on imported hardware and software and increases risks of cyber attacks [3].

For example, significant resources are spent on the Microsoft licenses required for the operation of applied information systems, as well as on licenses for foreign application software. A common practice is the use of software by various developers which increases information processing costs [4].

Due to the transition to electronic interaction between organizations and remote access to the consolidated resources of integrated structures, information leakage or distortion are possible. Most foreign software tools interact with the software manufacturer through global data networks, including when activating and verifying the validity of licenses, updating software. The access to files can be blocked after checking licenses. In addition, licensing agreements of Western system suppliers often impose a direct ban on the use of their software products for military purposes; in crisis periods, the technical support may be discontinued.

The ubiquitous use of imported telecommunication equipment and related software makes it difficult to ensure information security of control systems and protection against cyber threats when designing the latest products using digital models containing complete information about the products.

Consulting companies often defend interests of software suppliers, mainly foreign ones.

It is an urgent scientific task to develop modular protection of confidential information for instrument manufacturing enterprises whose main idea is to design a protection system from protection modules, inside
of which information is formed and transformed, and outside of the protection modules there are information threats. The shell of the modules should resist information threats.

It is assumed that information threats cannot arise inside the modules. Otherwise, the module affected by the information intrusion should be divided into two or more protected and secure modules with the distribution and modification of the information left from the broken module or the information processing should be stopped.

The protection modules interact; and the safe transfer of information from one module to another one is carried out. At the same time, information from a more secure module cannot be transferred to a less secure module if the level of confidentiality of the transmitted information prevents this.

Information can be transferred from a less secure module to a more secure module if the level of confidentiality corresponds to the degree of security of the transmitted module.

Depending on the level of confidentiality and the level of external threats, the protection module has an appropriate shell that allows you to perform tasks. The modular system of information protection allows various related enterprises to interact at the information level, provided that they have appropriate protection modules [5].

The merger, division, reorganization of enterprises is possible if there are indestructible interacting protection modules. In case of destruction or violation of the protective shell of the modules, the generation and transmission of information must be suspended, and these functions are transferred to other workable protection modules [6].

2. Information Threat Model for Instrument Manufacturing Enterprises

Specific products of the Instrument Design Bureau are scientific and technical information [7]. The development of methods for the creation, processing, transmission and storage of information by means of computer technologies generated threats caused by losses, modification and disclosure of data belonging to various subjects: developers and consumers of finished products and systems [8, 9].

2.1 The nomenclature, classification and specifics of information threats for instrument manufacturing enterprises.

The need to resist information threats is growing in the face of a weakly monopolized domestic and international market, when the level of competitive advantage of organizations and defense security of states depend on the degree of protection of confidential information [10].

Information threat is a possibility of an adverse event (impact, process or phenomenon) that can cause direct or indirect damage to the multilateral state of security of the instrument design engineering bureau during:
- development of new products and ensuring the rights to intellectual property;
- financing of scientific and technological developments and computer-aided design;
- domestic and interstate competition;
- counteraction to international intelligence structures;
- counteraction to national and international crimes and terrorism;
- defending their own reputation;
- exchange of scientific and technical information, etc.

There are a lot of information threats and their number is increasing. [11, 12, 13]

Figure 1 shows the general classification of information threats for a scientific-production system (design enterprises of the instrument-manufacturing industry) that uses computing tools and interacts with other similar scientific-production systems during the generation, modification, and exchange of confidential information. [14]
Fig. 1 General classification of information threats to the scientific and production system

Fig. 2. The simulation model of information threats for the design bureau
2.2 Purpose, structure, input and output data of the information threat model for design enterprises of the instrument-making industry

The model of information threats for design enterprises of the instrument-making industry is intended to formalize the type, intensity of manifestation and probability of the impact of a particular threat to the information system of the enterprise, as well as to determine the damage from the implementation of a particular threat to a given enterprise.

The model’s structure (Figure 2):
- The database of threats by their types and intensity;
- The generator of reproduction of threats with specified intensities;
- Changes of current threat parameters;
- Self-learning of information threats;
- The generator reproducing responses of the information security system to information threats;
- The registration of the status of security of the information system;
- The recording of damage to the system.

Input and output data:
Input data:
1. Threats by type, intensity of manifestation, potential damage to the system;
2. Probability of recognition of the types of threats.

Output data:
1. The amount of damage to the system from the types of threats;
2. Prevented damage to the system from the types of threats in response to the information security subsystem.

1.3 The algorithm of the simulation model of information threats

Step 1. The database on the types, intensity of manifestation of threats transmits information to the threat reproduction generator with specified intensity parameters.

Step 2. The generator of types of information threats is launched with the modified parameters of the types of threats.

Step 3. The generated threat parameters from the generator are fed to Block 6.

Step 4. The generator reproducing the response of the information security subsystem to information threats transmits information about probabilities of recognizing threats to Block 6.

Step 5. The security level of the system is checked. At a level higher than permissible (for example, 0.9), the conclusion is drawn: the system is protected (Block 8), otherwise it is not protected (Block 9).

Step 4. In the block registering the damage to the system, the damage to the system from the types of threats and the prevented damage to the system are calculated.

Step 5. In Block 4, new parameters of information threats are transmitted to Block 1 and Block 5.

3 Determination of security probabilities

To determine the probability of information security threats (P_i), the design enterprise needs to develop an effective information monitoring system that can monitor the intensity of various threats at various time intervals. The longer the observation intervals (t_n) and the higher the threat recognition efficiency, the more accurate the forecast for the next threat and the probability (P_i) of the threat.

The intensity of manifestation of a particular security threat to the system (λ_i) is equal to the ratio of the number of manifestations of such a threat (N_i) during the last observation period to the duration of the observation period of the threat (t_m):

$$\lambda_i = \frac{N_i}{t_m}$$  \hspace{1cm} (1)

The intensity of manifestation of a particular threat to security of the system can be expressed as a function of the number of manifestations of threats to the time the threat was being observed.

The number of manifestations of a particular threat to security of the system (N_{t_1, t_2}) is equal to the integral of intensity (λ_i) of manifestations of the threat from the observation time (t_m) in the current interval [t_1; t_2] of the duration of manifestation of the threat:

$$N_{t_1, t_2} = \int_{t_1}^{t_2} \lambda_i dt_m$$  \hspace{1cm} (2)
The probability of manifestation of the number $N \cdot t_1, t_2$ of certain security threats to the system $P (N \cdot t_1, t_2)$ in the current interval $[t_1; t_2]$ is calculated as follows:

$$P(N'_{t_1,t_2}) = \begin{cases} 1, & \text{если } N'_{t_1,t_2} \leq N_{t_1,t_2} \\ \frac{N_{t_1,t_2}}{N'_{t_1,t_2}}, & \text{если } N'_{t_1,t_2} > N_{t_1,t_2} \end{cases} \tag{3}$$

If the probability of one threat in the current interval $[t_1; t_2]$ is calculated as follows:

$$P(1) = 1, \text{если } N_{t_1,t_2} \geq 1 \tag{4}$$

If the enterprise does not have an effective information monitoring system, it cannot immediately calculate probabilities of information security threats. However, due to the accumulation of statistical data on threats, the accuracy of such calculations can increase.

To improve the effectiveness of the information monitoring system, an enterprise lacking experience in calculating the probability of threats should use the statistics of a similar enterprise.

It is important to assess the potential damage to the system caused by a specific threat.

The information processed by the system has a value that can be expressed in monetary units. This cost includes expenses for the development and subsequent modification of information (primary costs) $(M_a)$. For the production of serial samples of products developed on the basis of scientific and technical information, financial resources are used for production (production costs, $M_p$).

As a result of operation of new serial samples of instrument-making products, the level of security of objects with price $(M_p)$ should increase. Thus, the cost of primary and production costs is added to the cost of objects, which can be devalued if the enemy side reveals scientific and technical information during the implementation of a certain information threat in the system.

The damage prevented by the information security subsystem $(M_i)$ will be calculated as the product of recognition probabilities $(P_r)$ and counteraction $(P_c)$ of the threat from the information security subsystem and the sum of costs for developing and manufacturing new products and objects using new products:

$$M_i = P_r \cdot P_c (M_m + M_{a} + M_o) \tag{5}$$

If different $i$-types of threats are directed to various $j$-objects, in formula (2.5), the components are summed up:

$$M_i = \sum_{i=1}^{r} \sum_{j=1}^{H} P_{ri} \cdot P_{cj} (M_{mj} + M_{aj} + M_{oj}) \tag{6}$$

In special cases, if the developed objects are similar, or threats are similar, the summation by objects or threats is excluded from formula (2.6).

An additional tool for calculating the probability of information threats is a system simulating information threats, a training system for information monitoring of an enterprise whose elements are presented in Figure 2.2.

The system for simulating information threats can collect information on all potential threats that have ever occurred in the industry and generate threats for the enterprise being audited to evaluate the effectiveness of its information security system.

4. Conclusion

This article presents the nomenclature, classification and specifics of information threats to design enterprises of the instrument-making industry. The list of information threats and their expected consequences were formulated. The structure, input and output data of the simulation model of information threats were presented. Definitions are given and analytical expressions are suggested for calculating intensity of security threats; the amount of manifestation of a particular security threat in the time interval; the probability of occurrence of certain security risks was determined. The assessment of the potential damage to the system was presented given. The calculation of the prevented damage from activities of the information security subsystem was provided. The need of the subsystem for simulating information threats as part of the information security subsystem for design enterprises of the instrument-making industry was identified. The obtained data will be used for further work when designing the modular system for protecting the confidential information of a design enterprise of the instrument-making industry.
References

[1] Maksarov V V, Olt J, Krasnyy V A 2019 Investigation of wear resistance of bearing units engines of mining dump trucks operating in conditions of fretting corrosion *Journal of mining institute*, 235, 77 – 83

[2] Gerasimenko V A , Malyuk A A, 1997 Fundamentals of information security (Moscow: Moscow Engineering Physics Institute), 537

[3] Gromov Yu Yu, Drachev V O, Ivanova O G, Shakhov N G 2010 Information security and information protection: a training manual (Stary Oskol: TNT), 384

[4] Olt Y; Maksarov V V, Krasnyi V A 2018 Provision of adhesion strength of gasthermal coatings on piston rings of quarry transport engines *Journal of mining institute* 229 77-83

[5] Maksarov V V, Olt J 2017 Dynamic stabilization of machining process based on local metastability in controlled robotic systems of cnc machines *Journal of mining institute* 226 446-451

[6] Maksarov V V, Olt J. 2015 Improving the precision of manufacturing power hydraulic cylinders of powered roof supports based on a vibration-damping tooling system *Journal of mining institute* 214 71-84

[7] Yablochnikov E I, Molochnik V I, Fomina Yu N 2008 Reengineering of business processes of design and production / Textbook (St. Petersburg: St. Petersburg National Research University of Information Technologies, Mechanics and Optics) 152

[8] Alekseenko V N, Dreve Yu G 1996 Fundamentals of building protection systems for industrial enterprises and banks: a manual (Moscow: Moscow Engineering Physics Institute).

[9] Prokhorov S A, Fedoseev A A, Iwashchenko A V 2008 Automation of integrated enterprise security management (Samara: Saratov Scientific Center of the Russian Academy of Sciences) 55

[10] Krasnyy, V A, Maksarov, V V, Olt, J 2015 The use of polymer composite materials in the friction nodes downhole oil pumps *Journal of mining institute* 211 71-79

[11] Malyuk A A 2004 Information security: conceptual and methodological foundations of information security. Textbook manual for universities. (Moscow: Hotline - Telecom) 280

[12] Ignatiev V A 2005 Information security of a modern commercial enterprise: Monograph (Stary Oskol: TNT LLC) 448

[13] Saderdinov A A, Traynev V A, Fedulov A A, 2004 Information security of an enterprise: Textbook. - 2nd ed. (Moscow, Publishing and Trading Corporation "Dashkov and Ko") 336

[14] Shangin V F 2013 Information security of computer systems and networks: a training manual (Moscow: Publishing House “FORUM”: INFRA-M) 416