Models of Optimizing the Information Security Industry Infrastructure

Lilia Aubakirovna Enikeeva

Doctor of Science, professor of The Operations Research in Economics Department (Professor Y.Lvov Department)
Saint-Petersburg State University of Economics, Sadovaya, 21 St. Petersburg
Enikeeva_lilia@mail.ru

Elena Victorovna Stelmashonok

Doctor of Science, professor of The Computer Systems and Programming Department
Saint-Petersburg State University of Economics, Department of Sadovaya, 21 St. Petersburg
vitaminew@gmail.com

Vitali Leonidovich Stelmashonok

Ph.D., assistant professor of The Management organization Department
Saint-Petersburg State University of Economics Sadovaya, 21 St. Petersburg
stelmashonok@gmail.com

Doi:10.5901/mjss.2015.v6n5p353

Abstract

In the context of systematic instability increases the dependence of national economies on the degree of information technology security, information security risks related to the growth of internal and external attacks targeted at the business of industrial enterprises appear. As a result, the core business processes of industrial enterprises are being affected: stopping or interruption of the operation of systems and services; damage, loss or compromise of data; direct financial losses as a result of illegal actions of internal staff and cybercriminals. According to Gemalto (Information Security, 2015) the number of data breaches in 2014 increased by 49% compared to 2013 year, and about one billion records were compromised for the purpose of identity theft. The situation is critical in all industries and sectors. Implementation of Information Security Management System is aimed at the systematic identification, analysis and mitigation of information security risks as a result of which information assets are losing confidentiality, integrity and availability.

Keywords: *information security risks of information infrastructure, information infrastructure protection, infrastructure optimization model of information security, the protection of information resources.*

1. Introduction

In information economy, information technologies become a compulsory part of business processes of industrial enterprises, therefore increasing their dependence on the security degree in information technology.

The information systems of an industrial enterprise are requirements in the field of information security and business continuity. Information infrastructure provides secure data processing and information support of business processes within an industrial enterprise and exchange of information resources with the environment.

This article focuses on the modeling of information security infrastructure of industrial enterprises using the apparatus of linear programming to optimize it. It provides a solution to the problem of optimizing protection of information infrastructure of an industrial enterprise in the form of complex mathematical models that include both a model for minimizing the cost of optimizing infrastructure information protection and maximization model quality infrastructure protection information. Sources for this article became years of research materials of its authors and publications in the public domain.

2. Material and Methods

The main approaches used are a systematic approach and process-oriented approach to information security management of an industrial enterprise, have been actively used by Russian and foreign researchers, as well as methods

and linear programming model to assess strategies for the protection of information on industrial sites.

The used materials and sources in complex will allow to solve tasks. The work is based on materials and data published sources.

3. Results

Analysis of the dynamics of attacks and potential threats to information security has shown that the development of information security management systems is of strategic importance for the development of the national economy of Russia.

Information Risk Management is part of the overall management system which is based on a process-oriented approach to the creation, implementation, operation, monitoring, analyzing, maintaining and improving information security of industrial enterprise.

Proposed in the article Infrastructure Optimization Model of information security of industrial enterprise can reduce the optimization cost of information infrastructure protection and improve the quality of information security infrastructure.

Maintaining the stability of the control system of industrial enterprise is impossible without security assessment of business processes of industrial enterprises.

4. Discussion

Information infrastructure of industrial enterprises includes a set of software and hardware tools, organizational and administrative measures to ensure the safe handling of combined data and information support of business processes within industrial enterprises, as well as adequate opportunity to exchange information with the external environment.

In the article the authors under the information infrastructure term understand a set of standard technological elements, tools and techniques that are, on the one hand, do not depend on the specific problem to be solved, but on the other hand, are easily joined together and have the means to integrate with existing «legacy» subsystem (Stelmashonok E.V. and Enikeeva L.A., 2006). Information infrastructure of the industrial enterprise enables reliable operation and interaction of all members of the information system of functional modules and application subsystems, to present a set of necessary tools and instruments to manage the system, its maintenance and development (Dyatlov S. A. and Selishcheva T. A., 2014).

As part of the information infrastructure of industrial enterprises it is necessary to create a well-working infrastructure protection information, business processes, to ensure the continuity of business processes. Figure 1 shows the infrastructure of information security systems business processes of industrial enterprises, the mechanism of the system' elements interaction: protection against unauthorized access, interception of the information transmission from random noise and disruption from the information intervention into business process (Stelmashonok E.V., Tarzanov V.V. and Stelmashonok V.L., 2011).

Protection of information resources, primarily directed against various types of threats. Information resources may be at risk (Stelmashonok E.V. and Enikeeva L.A., 2006):

- unauthorized access to confidential data from both outside and inside the structure, their selfish use and disclosure;
- interseption, substitution and distortion of information during transmission;
- aimed misrepresentation, falsification or substitution of data to unauthorized access;
- information intervention in the business process.

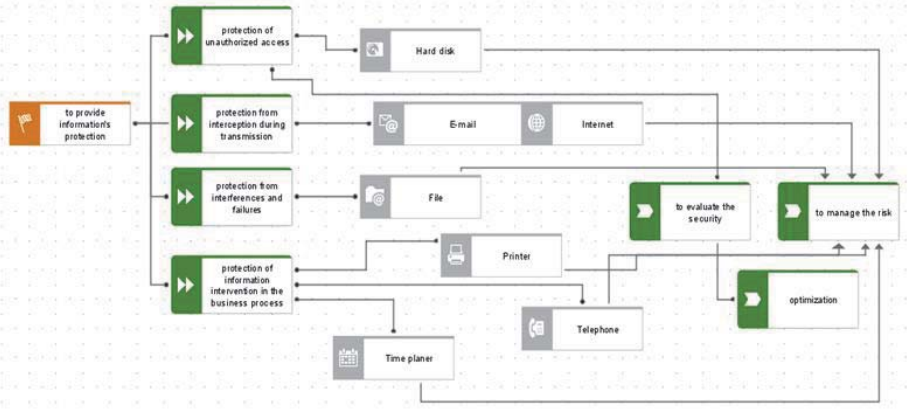

Figure 1. Infrastructure information protection system of business processes

The problem of optimizing the information security industry infrastructure may be presented in the form of complex mathematical models, including:

- model of minimizing the cost of optimizing infrastructure protection;
- model of maximizing the quality of information security infrastructure.

Suppose that (1) R – composite index assessing the quality of the information infrastructure protection (generalized coefficient of security, showing the level of reflection attacks on the totality of possible threats), where:

r_i – private indicator assessing the quality of the infrastructure of information security (private security factor, showing what part of the threat i is recognized);

N – the set of indicators to measure the quality of private, reducible to the generalized indicator;

K_i – - weighting of private quality index. i in the additive convolution.

$$R = \sum_{i \in N} K_i \cdot r_i \qquad (1)$$

$$\sum_{i \in N} K_i = 1 \quad , \qquad (2)$$

Compliance with conditions (2) prevents the possibility of unlimited compensation of insufficient value of a private performance by the other. If this condition is not met, the convolution is performed and a general indicator is equal to zero.

Aiming of the optimization problem of information security infrastructure is as follows (Stelmashonok E.V, 2006):

Model minimize infrastructure costs of information security. This model can be represented as integer programming problem with boolean variables.

Required to minimize the cost of inputs:

$$S = \sum_{i \in I} \sum_{j \in J} S_{ij} \cdot x_{ij} + \sum_{i \in I} S_i \cdot y_i \to \min \qquad (3)$$

subject to certain restrictions:

$$\sum_{i \in I} \sum_{j \in J} a_j r_{ij} x_{ij} \geq R_{dop} \qquad (4)$$

$$\sum_{i \in I} x_{ij} = 1 \quad , \forall j \in J \qquad (5)$$

$$y_i = \begin{cases} 1, \sum_{j=1}^{J} x_{ij} > 0 \\ 0 \end{cases} \qquad (6)$$

$$x_{ij} \in \{0;1\} \qquad (7)$$

where:

S_{ij} –the cost of protecting information assets j, funds i;

S_i –costs associated with the protection of information assets means i;

I –the set of information security;

J –the set of protected information assets;

r_{ij} –assessment of the quality of protection by means i of information assets j;

a_j –weighting factor information asset j in the overall assessment of the security infrastructure of information, $\sum_{j=1}^{J} a_j$;

R_{dop} – acceptable level of quality infrastructure protection information in general;

y_i – binary variable that takes the value $y_i = 1$, if the data protection tool i can be used in infrastructure protection information differently $y_i = 0$;

$x_{ij} = 1$, if the developer chooses data protection tool i for protecting information assets j, differently $x_{ij} = 0$.

In the *model of maximizing the quality level of information security infrastructure* (Stelmashonok E.V, 2006) criterion is to maximize the quality level of information security:

$$R = \sum_{i \in I} \sum_{j \in J} a_j r_{ij} x_{ij} \to \max \quad (8)$$

In this model, the level of quality of infrastructure protection information is maximized under the following restrictions:

$$S = \sum_{i \in I} \sum_{j \in J} S_{ij} x_{ij} + \sum_{i \in I} S_i y_i \le S_{dop} \quad (9)$$

$$\sum_{i \in I} x_{ij} = 1, \quad \forall j \in J \quad (10)$$

$$y_i = \begin{cases} 1, \sum_{j=1}^{J} x_{ij} > 0 \\ 0 \end{cases} \quad (11)$$

$$x_{ij} \in \{0;1\}, \quad (12)$$

where S_{dop} - the allowable cost of information security systems.

It is advisable to share the proposed models. So, when restricted to the allowable costs of protection, the maximum value of the quality of the infrastructure of information security can be found. In some cases, this may have not one but several solutions (security profiles). To choose the solution from among the found optimal solutions, which requires minimal protection, the second problem should be solved. As a limitation factor found in the first problem the importance of quality infrastructure protection information should be present.

Optimal cost security system is not the most secure.

The concept of cost-optimal information security system is of limited use. It is possible that, regardless of the value of information security systems, the likelihood of injury remains constant or has even a positive value (due to the increased vulnerability of the protection system). In the latter case there is a question about the refusal of information security systems.

In the information security management system of industrial enterprise the risk management system is less studied and requires separate consideration.

The process of information security risk management involves the following steps (Figure 2): planning, implementation, verification, improvement and implementation of the following procedures.

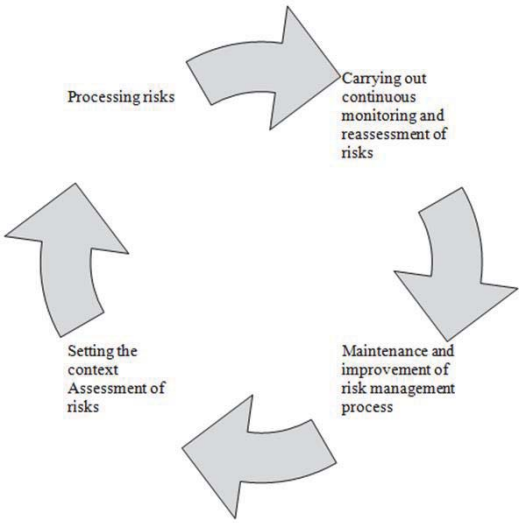

Figure 2. The process of managing information security risks

Criteria for assessing information security risks should take into account the strategic value of information assets, information security from the perspective of confidentiality, integrity and availability. At the planning stage the context definition is to formulate goals information security risk management, development of criteria for accepting risks and determining acceptable levels of risk (Stelmashonok E.V., 2012 and Selishcheva T. A., 2014).

In addition, in determining the context of the enterprise should evaluate whether there are adequate resources for:

- implementation risk assessment and creation of a plan for handling risks;
- finding and implementation of policies and procedures, including the implementation of the selected measures and tools for monitoring and control;
- implementation monitoring measures and tools for monitoring and control;
- implementation monitoring of information security risk management.

Including the analysis of:

- classification level of information assets at risk;
- the most probable threat of information security violation (integrity, availability and confidentiality of operational activities of industrial enterprises);
- financial losses assessment alleged damage to reputation.

The risk assumption refers to the admission of the existing level of risk, ie industrial enterprise allows the probability of possible negative consequences.

It is necessary to consider the following:

- risk taking criteria may include some of the thresholds specified when the desired target level of risk, with the caveat that under certain circumstances, top management will take risks that are above that level;
- risk taking criteria can be expressed as the ratio of profit quantified (or other business benefits) and quantitatively assessed risk;
- different classes of risks may apply different criteria for risk-taking. For example, can not accept the risks associated with the legal requirements, at the same time a high level of risk-taking may be permitted, if it is determined by contractual obligations;
- risk taking criteria may include requirements for additional processing risk in the future. For example, the risk may be accepted if pledged to take measures to reduce the level of risk for a certain period of time;
- risk acceptance criteria may vary depending on how long there will be a risk of expectation, for example, if it is associated with a short or long-term operations;
- risk taking criteria take into account the criteria established businesses, especially legislation, operations, technology, finance, social and human factors.

Risk assessment (risk assessment) - the overall process of risk analysis and assessment is presented in Figure 3.

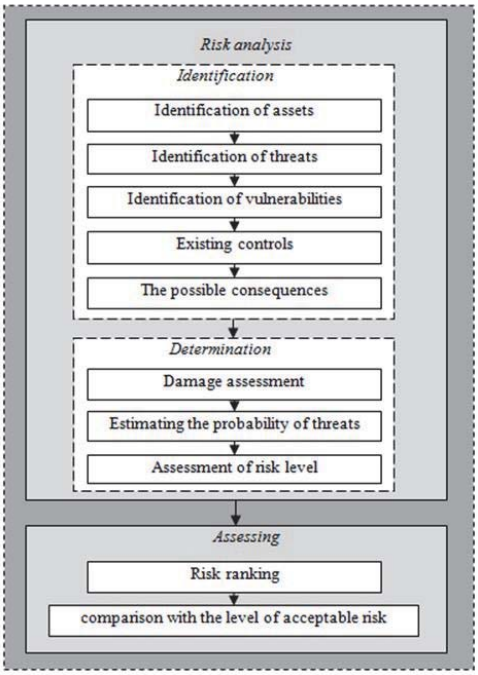

Figure 3. The main stages of risk assessment

Risk analysis (risk analysis) - the systematic use of information to identify sources of risk and determine its value.

Risk analysis consists of procedures:

- risks identification, including the identification of assets , these assets threats, the vulnerability of assets , which can be used as threats, existing controls and the possible consequences (potential consequences) impact on the assets as a result of threats to information security;
- find risk value (risk estimation) - involves assigning values to the probability and consequences of risk.

At this stage, the estimated:

- damage (negative effects, impact) for the company's main activity, which may be caused as a result of the possible implementation of information security threats;
- probability (likelihood) of threats, taking into account existing vulnerabilities of assets and measures used to protect information;
- risk-levels.

Information resources may be at risk:

- the reduced data transmission systems inoperable as a result of malicious or careless actions, for example, by overloading useless information ("spam");
- unauthorised access to confidential data from both outside and inside the structure, their selfish use and disclosure;
- aimed misrepresentation, falsification or substitution of data to unauthorized access;
- substitution and distortion of information provided to the public.

5. Conclusions

In conclusion, the models of information security can reduce the cost of infrastructure of information's protection, can improve the quality of infrastructure of information's protection and evaluates the security of the business processes of industrial enterprises.

Implementation of the system will reduce the risks that result in information assets lose the confidentiality, integrity

and availability.

References

Gemalto: leak for 2014 // Information Security. 2015. №1. (In Russian).

Dyatlov S. A. and Selishcheva T. A., 2014. The new role and functions of the global innovation hypersecreted companies in the modern economy. RUDN Vestnik, 3:127-135. (In Russian).

Selishcheva T. A., 2014. Spatial disparities informatization of the Russian economy. Science and practice, 1(13): 69-73(In Russian).

Stelmashonok E.V. Organization of information security business processes. // Applied Informatics. 2006. № 2, p. 42-57. (In Russian).

Stelmashonok E.V., Broido V.L., Bugorsky V.N. et al., 2012. Safety of modern information technologies: a monograph. St. Petersburg. (In Russian).

Stelmashonok E.V., Tarzanov V.V. and Stelmashonok V.L., 2011. Modelling of correlating threats of information safety of enterprise. ENGEC Vestnik, 5 (48): 175–181. (In Russian).

Stelmashonok E.V. and Enikeeva L.A., 2006. Information risks management as a basis for a stable (sustainable) company development. STU Scientific and technical statements, 43: 146–149. (In Russian).