ATLANTIS PRESS
Advances in Computer Science Research (ACSR), volume 72
IV International Research Conference "Information Technologies in Science, Management, Social Sphere and Medicine" (ITSMSSM 2017)

Model of enterprise's information security management

Tatiana Omelchenko, Mikhail Umnitsyn, Arina Nikishova, Natalia Sadovnikova
Department of Information Security
Volgograd State University
Volgograd, Russia
omelchenko.tatiana@volsu.ru, umnitsyn@volsu.ru, nikishova.arina@volsu.ru, sadovnikova.natalia@volsu.ru

***Abstract*—The problem of constructing of information security management system, taking into account the scale and structure of the enterprise, is considered. The main models used for solving problems of enterprise's information security management are analyzed. The main shortcomings and problems of their application are determined. The model that takes into account the specifics of enterprise's operation and allows to carry out management of various information security tools for various types of enterprise assets and threats to information security, is proposed. The software package that implements the model is developed. With help of software package experimental studies on typical automated control system of technological processes of the enterprise are carried out.**

Key words—information security management, automated control system of technological processes of the enterprise, enterprise asset, information security tool, threat to information security, threats' to information security management.

I. INTRODUCTION

The greatest importance for the modern enterprises is the security of their technological processes. Currently, the complexity of these processes is so great that most enterprises use automated control system of technological processes (ACS TP). Any adverse impact on such a system is unacceptable.

According to the statistics of Positive Technologies [1] the list of major relevant ACS TP threats is identified (Fig. 1). Today components of ACS TP are used in a variety of areas, from nuclear power plants to personal systems of "Smart home". Accordingly, if an intruder discovers vulnerability in one component of ACS TP, he will be able to carry out attacks on many objects throughout the world.

The growth of amount of threats, the diversity of information security tools, the complexity of technological processes of the enterprise leads to necessity of information security management system (ISMS) application. Enterprise is usually oriented to one of the existing information security management standards, when building ISMS.

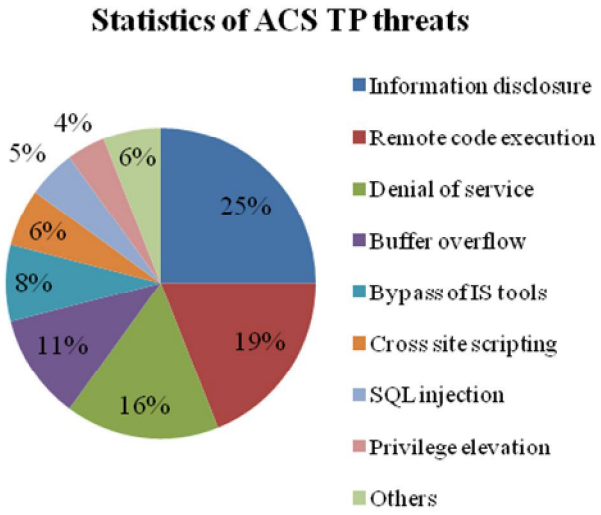

Fig. 1. Relevant ACS TP threats.

According to [1] it is required to consider purpose and need, scope of operation and structure of the enterprise. For the development, implementation and functioning, monitoring and improving of ISMS of an enterprise, the process approach should be used. The integration is made at all stages: planning (development of ISMS), implementation (integration and operation of ISMS), check (monitoring and analysis of ISMS), act (maintain and improve of ISMS). According to the requirements of [2], information security management must be performed in accordance with business requirements and relevant laws and regulations, with the support of senior management.

A special place in this family of standards holds [3]. It implies the use of methods that allow you to balance the time and effort spent on the choice of measures and means of information security for action of enterprise's information security management with support of high-level risk assessment (Fig. 2).

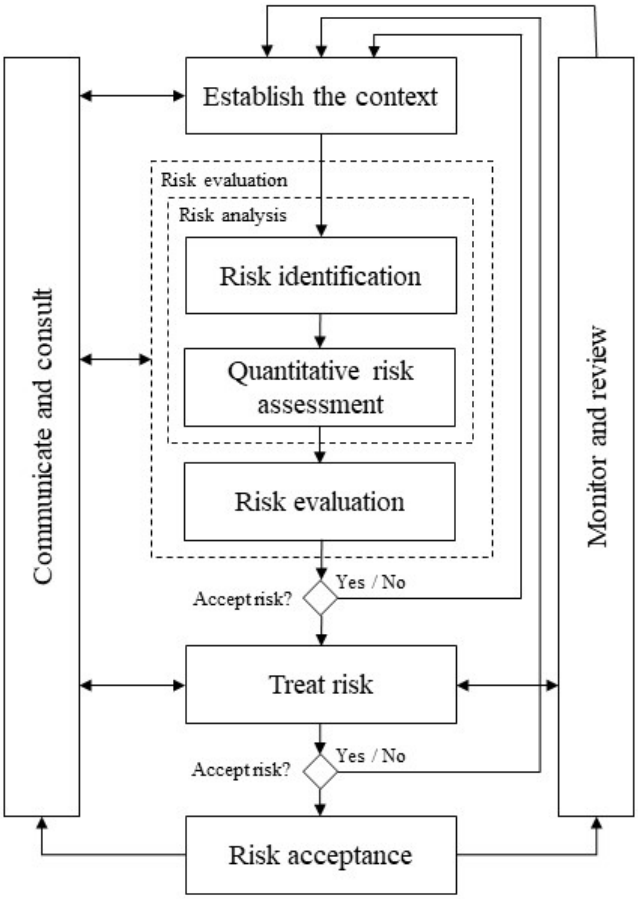

Fig. 2. Process of IS risk management.

Implementation of ISMS according to family of ISO/IEC 27000 requires to take into account the many other references and standards, for example, family NIST, FIPS for foreign organizations or the observance of FSTEC orders [4]. In this case problems presented in Table 1 occurs.

TABLE I. PROBLEMS OF ISMS IMPLEMENTATION IN ACS TP

Characteristic	Problems
Number of external requirements 253–FL, the order of FSTEC of Russia No. 31, industry requirements, NIST, CIPNERC, etc.	• Overlapping requirements • Costs of compliance
Integration with corporate management system Purposes, risks, etc.	• Demonstration of the results • Accuracy of the estimates
Extensive scope People, branches , processes, ACS TP, IS, etc.	• Monitoring of implementation • Assessment of the current state
The amount of information Sources – ISS, ACS TP, people, etc. Storage – DB, files, folder, etc.	• Relevance of the information • Search and reporting

The implementation of ISMS according to standards is not a universal solution. This is a complex procedure, requiring changes of enterprise's technological processes.

Thus, the main goal of building of ISMS is to assess and retention of risk values in acceptable to enterprise range. Therefore, the managed objects are the risks of the enterprise, and the managing body is the protective measures. Management system must provide the choice of optimum protective measures that ensure protection of the enterprise's assets from information security threats.

The model ISMS includes the following processes:

- asset management;
- information security risk management;
- information security tools management;
- change management;
- informing and education management;
- incident management;
- documents management;
- roles management;
- staff management;
- business continuity management;
- operating efficiency management;
- control activities management.

The main and most important processes are the first three processes. The relationship of these processes are cyclical (Fig. 3).

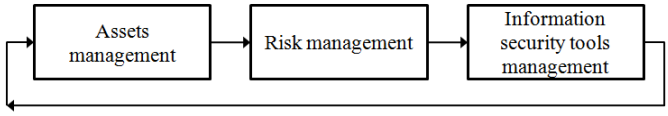

Fig. 3. Connection between main processes of ISMS.

II. THE EXISTING APPROACHES TO ENTERPRISE'S INFORMATION SECURITY MANAGEMENT

In article [5], the author comes to the conclusion that building ISMS is often based on appropriate standards, which provides only general information without giving specific project. The author defines the requirements for modern ISMS and proposes a project based on the theory of the survivability of the system.

The disadvantage of proposed model is that ISMS built on its basis does not consider all of the threats to information security. Also there is no ISMS dependence on ACS TP of enterprise.

The author of work [6] proposes to use his developed frame ADAMANT to improve the automation of the information security management process. Also management process takes into account the value of information security risks.

The disadvantage of this approach is the limitation of the developed ISMS structure and capabilities according to the proposed framework. Also not all functions of information security management are taken into account, but only risk management.

In [7] the approach to protective measures management based on their efficiency rate is proposed. Weight function to evaluate the effectiveness of the information security system is designed. The basis of weight function is number of criteria reflecting the probability of occurrence and counter the threat and degree of its danger. The proposed weighting function has the property of accumulation in case of repelling threats and allows to evaluate the effectiveness of the information security system. Modeling security threats should reflect the dynamic state of the information security system. The model is based on the colored Petri nets.

The disadvantages of this model are its computational complexity and the presence of information pre-collection and gathering stage before ISMS can start functioning.

In [8] the features of the regression analysis in ISMS use are considered. The analysis of the advantages and disadvantages of the regression analysis methods applied to the assessment of the security breach risks is carried out. Attention is paid to the specific use of regression analysis to ensure the adequacy of the applied models when assessing the security breach risks. The conditions for obtaining the desired results when building a regression model are defined. The features of the states prediction when using regression analysis are considered. Recommendations for the use of regression analysis for estimating the information security breach risk are proposed.

The disadvantage of this approach is its computational complexity, and the need to collect statistical data for the functioning of ISMS.

Given the shortcomings of analyzed models, the model of enterprise's information security management is proposed.

III. Mathematical Model of Enterprise's Information Security Management

The process of enterprise's information security management can be described as a combination of the following functions (1):

$$F_u = F_u(f_{ua}, f_{ur}, f_{zm}), \quad (1)$$

where f_{ua} – function of enterprise assets management, f_{ur} – function of enterprise's information security risks management, f_{zm} – function of information security tools management.

The process of assets management, in turn, is described by a function of three main elements (2):

$$f_{ua} = (C_i, S_i, V_i), \quad (2)$$

where C_i – category of *i*-th asset, S_i – value of *i*-th asset, V_i – nature of impact on *i*-th asset.

The value of the asset category belongs to the set (3):

$$C_i = \{O, D\} \quad (3)$$

where O – category of main assets, which are understood as technological processes and information, D – category of secondary (supportive) asset, which is understood as hardware, software, net, staff, place of enterprise's functioning, enterprise's structure.

To determine the value S_i of *i*-th asset, it is needed to determine grading scale, that allows to organize assets according to their values. Scale for assets of ACS TP value expressed in qualitative and quantitative form presented in Table 2

TABLE II. SCALE FOR ASSETS OF ACS TP VALUE EXPRESSED IN QUALITATIVE AND QUANTITATIVE FORM

Value of asset S (quantitative form)	Value of asset S (qualitative form)
(0 – 2)	Very low
[2 – 4)	Low
[4 – 6)	Medium
[6 – 8)	High
[8 – 10]	Very high

The IS incident may impact more than one asset or only a portion of the asset, depending on the success of the IS incident. There is an important difference between the value of the asset and influence stemming from the incident. The impact is considered as having immediate (operational) effect V_o, or a future (business) effect V_b, which includes the financial and market consequences (4).

$$V_i = \{V_o, V_b\} \quad (4)$$

Operational influence may be direct P or indirect K (5):

$$V_o = \{P, K\}, \quad (5)$$

where

$$P_i = \langle fc_i, cp_i, cpi_i, ib \rangle$$

where P_i – direct influence on *i*-th asset, fc_i – financial replacement value of lost *i*-th asset (portion of *i*-th asset), cp_i –cost of acquisition, configuration and installation of new *i*–th asset, or a backup, cpi_i – cost of suspended because of the incident operations, while the service provided by the *i*–th asset(s), will not be restored, *ib* – influence, leading to violation of IS.

$$K_i = \langle uv_i, po, zi, no, en \rangle$$

where K_i – indirect influence on *i*-th asset, uv_i – costs of lost opportunities (financial resources required to replace or restore of *i*-th asset), *po* – cost of interrupted operations, *zi* – possible misuse of information obtained as a result of a security breach, *no* – violation of statutory or regulatory obligations, *en* – violation of the ethical rules of conduct.

After studying the available assets and determine how valuable they are to the enterprise, it is needed to determine the overall level of acceptable risk. At this stage the function of enterprise's information security risks management is implemented (6).

$$f_{ur} = f_{ur}(P_{ug}^{i}, P_{es}^{j}, S), \quad (6)$$

where P_{ug}^{i} – probability of occurrence of the *i*–th threat, P_{es}^{j} – efficiency of the *j*–th information security tool (7).

$$P_{es}^{j} = 1 - P_{sz}^{j}, \quad (7)$$

where P_{sz}^{j} – probability of overcoming the *j*–th information security tool, S – asset value.

Well-chosen level of acceptable risk and, consequently, the acceptable level of safety are key elements of successful safety management in implementation of function of information security tools management f_{zm}. The managed objects are risks, and management bodies are information security tools. Function of information security tools management should ensure the selection of adequate information security tools that ensure the safety of information assets from possible threats.

Under the effective management of information security tools the information security system is at the highest possible level of utility. It can be obtained with the most efficient use of currently available tools. So the following optimization problem is put (8):

$$\begin{cases} Efficiency\ of\ ISS \to max \\ Risk \to min \\ Cost\ of\ ISS \to min \end{cases} \quad (8)$$

If not one, but several criteria of optimality are specified, then for definiteness for each of them it must be specified the "direction of interest" of decision makers (DM) as in Table 3.

TABLE III. DIRECTION OF INTEREST OF DM FOR CRITERIA OF OPTIMALITY

Quantitative form	Efficiency of ISS	Risk	Cost of ISS
(0 – 2)	Very low	Very high	Very high
[2 – 4)	Low	High	High
[4 – 6)	Medium	Medium	Medium
[6 – 8)	High	Low	Low
[8 – 10]	Very high	Very low	Very low

For this reason further consideration is restricted to the case when the decision maker is committed to getting possible large values of all the components of the vector criterion *f*. This fact can be expressed in terms of the so-called axiom of Pareto.

For all pairs of feasible solutions $x', x'' \in X$, for which we have the inequality $f(x') \geq f(x'')$, performed ratio $x' \phi x''$.

In the framework of the task of information security management the set X represents the set of possible sets of information security tools. According to the given optimization problem, a vector criterion has the form $f(x) = (E, R, C)$, where E – efficiency of ISS, R – risk, C – cost of ISS.

The comparison of two vectors is reduced to comparisons of their lengths (9).

$$f(x') \geq f(x'') \to |f(x')| \geq |f(x'')|. \quad (9)$$

The formula for calculating the length of a vector has the form (10):

$$|f(x)| = \sqrt{E^2 + R^2 + C^2}. \quad (10)$$

Since the lengths of the vectors belong to the set of real numbers, then by pairwise comparison of the lengths of the vectors can be replaced by finding the maximum value on the set of the lengths of the vectors for the set X as in (11).

$$\max(|f(x)|), \forall x \in X. \quad (11)$$

Found set of information security tools is Pareto optimal.

The proposed mathematical model is implemented in software package.

IV. EXPERIMENTAL STUDIES

Experimental study on simulated model of ACS TP of enterprise were carried out. The initial data for the experimental studies were: set of assets and their values; set of threats and probability of their realization; set of information security tools to block threats, of which the subset of the installed tools is highlighted. To determine the probability of threats realization available statistical data is used.

Priori risk of information security is estimated in experiments using the developed software package. Then the problem for the effective information security tools management is solved. And the re-assessment of risk is carried out.

Pre-populated database contains following tables: «Assets», «Threats», «Tools».

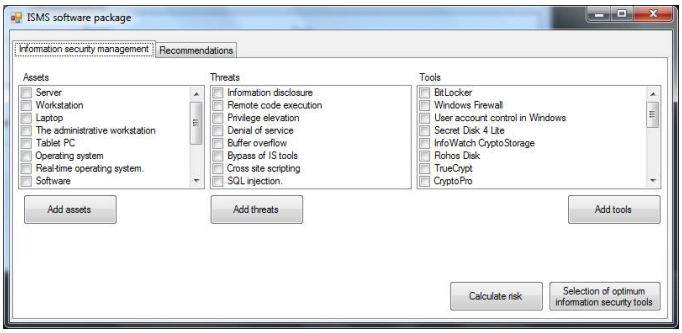

Fig. 4. Display of received data from tables: assets; threats; tools.

For the first experiment the asset “Server” and the threat “Information disclosure” is chosen. Also the information security tool “BitLocker” is selected (this tool is taken for pre-installed in the enterprise).

After pressing the button “Calculate risk”, we get: value of risk – 0,134757.

After pressing the button "Selection of optimum information security tools" we receive: Pareto optimal tool for protection against threat of "Information disclosure" – "CryptoPro" (Fig. 5).

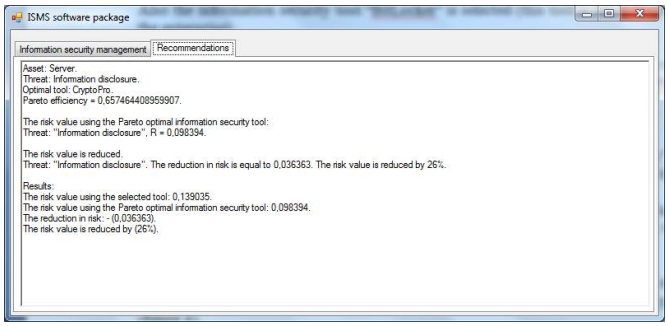

Fig. 5. Results of software package work.

The risk value using the Pareto optimal information security tool “CryptoPro” – 0,098394; Pareto efficiency– 0,657464408959907. The reduction in risk is equal to 0,036363. The risk value is reduced by 26%.

For the second experiment the asset “Server” and the threat “Remote code execution” is chosen. Also the information security tool “Windows Firewall” is selected (this tool is taken for pre-installed in the enterprise).

After pressing the button "Calculate risk", we get value of risk – 0,074175.

After pressing the button "Selection of optimum information security tools" we receive: Pareto optimal tool for protection against threat of "Remote code execution" – " Cisco ASA 5505" (Fig. 6).

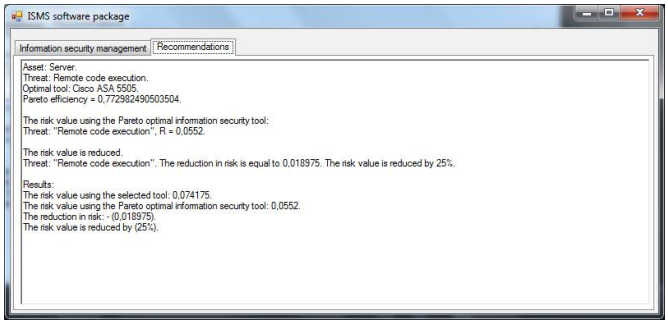

Fig. 6. Results of software package work.

The risk value using the Pareto optimal information security tool “Cisco ASA 5505” – 0,0552; Pareto efficiency– 0,772982490503504. The reduction in risk is equal to 0,018975. The risk value is reduced by 25%.

For the third experiment the asset “Server” and the threat “Privilege elevation” is chosen. Also the information security tool “User account control in Windows” is selected (this tool is taken for pre-installed in the enterprise).

After pressing the button "Calculate risk", we get: value of risk – 0,04278.

After pressing the button "Selection of optimum information security tools" we receive: Pareto optimal tool for protection against threat of "Privilege elevation" – "Secret NET" (Fig. 7).

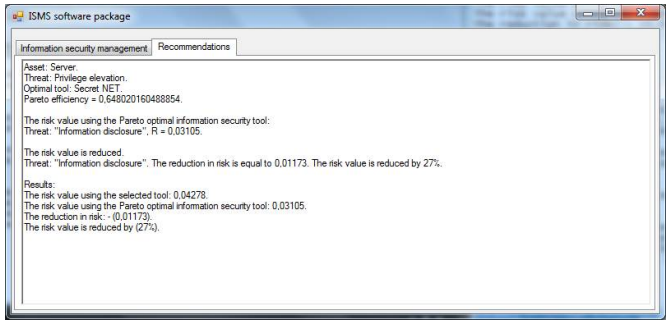

Fig. 7. Results of software package work.

The risk value using the Pareto optimal information security tool “Secret NET” – 0,03105; Pareto efficiency – 0,648020160488854. The reduction in risk is equal to 0,01173. The risk value is reduced by 27%.

V. Conclusion

According to the results of experimental study the diagram is drawn (Fig. 8).

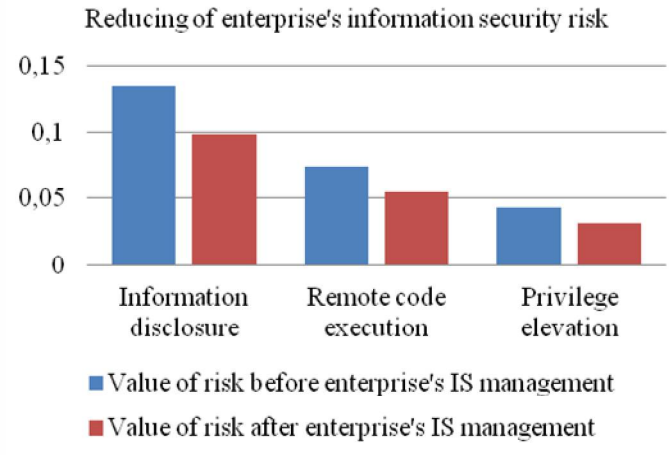

Fig. 8. Change of risk value using the optimum information security tools.

The results show that the use of Pareto optimal information security tools for the selected threats allows to reduce information security risk by an average of 26%.

Developed a software package does not have large computational complexity and is flexible, allowing to obtain a risk assessment and manage various information security tools for various types of enterprise assets and threats to information security.

REFERENCE

[1] "ICS security: 2016 year in review", Positive Technologies, 2017, pp. 3-4. URL: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/ICS-Security-eng.pdf

[2] ISO/IEC 27001:2005. Information technology — Security techniques — Information security management systems — Requirements (IDT)

[3] ISO/IEC 27002:2005. Information technology. Security techniques. Code of practice for information security management.

[4] ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management.

[5] S.T. Arnason, K. D. Willett. "How to Achieve 27001 Certification: An Example of Applied Compliance Management", CRC Press, 2007, pp. 5-12.

[6] S. Goldes, R. Schneider, C. M. Schweda, J. Zamani. "Building a viable information security management system". 3rd IEEE International Conference on Cybernetics, CYBCONF 2017; Exeter; United Kingdom; June 2017.

[7] M. Brunner, C. Sillaber, R. Breu, "Towards automation in information security management systems", 17th IEEE International Conference on Software Quality, Reliability and Security, QRS 2017; Prague; Czech Republic; July 2017, pp 160-167.

[8] A.P. Gorlov, M.Y. Rytov, V.T. Eremenko, "Automation of the process of assessing the security state of Informatization object by using colored Petri nets from information leakage", Information and security, vol. 1, 2015, pp. 123-126.

[9] A.B. Los, A.S. Kabanov, "Features of information security risk evaluation using regression analysis in the information security management system.", Industrial ACS and controllers, vol. 1, 2014, pp. 58-66.