International Review of Management and Marketing

ISSN: 2146-4405

available at http: www.econjournals.com

International Review of Management and Marketing, 2016, 6(S5) 125-135.

Models of Complex Industrial Facilities Assessment Based on Risk Approach

Livshitz Ilya Iosifovitch, Lada Avenirovna Podolyanets*

National Mineral Resources University (University of Mines), 2, 21 Line, 199106 St. Petersburg, Russia.
*Email: podolyanets@mail.ru

ABSTRACT

The problem of forming models for providing complex industrial facilities (CIFs) assessment is relevant because different slants to forming IT-security management systems (ISMSs) budget are exist. The models of CIFs assessment based on risk-based approach for fuel and energy complexes and airport complexes, and importance of realization the Plan-Do-Check-Act cycle noted. This approach increases speed of IT-security audits process, increase the reaction from management and increase the total IT-security level. It is shown that an ultimate goal of application setting of IT-security controls is decreasing potential damage concerning the chosen assets of CIFs. The received results can find application during the full lifecycle including forming, assessment and optimization of the IT-ISMS and budget justification. Application of the received results can be demanded when forming models and methods of internal audit and monitoring the objects being under influence of threats of IT-security violation.

Keywords: Audit, Information Security, The Integrated System of Management, Risk Management
JEL Classifications: G32, L15, M15

1. INTRODUCTION

Safety of the complex industrial facilities (CIFs) represents a relevant problem, constant consideration of experts and the highest management to which is caused by system questions – both external and internal genesis. We understand CIF as "technical object, for which the unauthorized change of the regular mode of functioning connected with violation of properties of information security lead to threat of techno-genic catastrophes with irreversible consequences" (Federal Law of Russian Federation 256-FZ 2011, July 21). The main difficulties of formalization of requirements for CIF are divided into two aspects: The technical – actually management of means of ensuring of IT-security (a problem of productivity) and economic – ensuring balance of cost of IT-security system in relation to the cost of the protected object (a problem of efficiency). Some questions of management of technical and economic security of structural and difficult systems based on logic-probabilistic models are considered in Solozhentsev and Ryabinin's works (Solozhentsev, 2014; Solozhentsev, 2011; Ryabinin, 2007).

The technical aspect is rather fulfilled now – A complex of measures is aimed at providing IS (in the notation of ISO – "asset"), that accepted to unite in the uniform IT-security management system (ISMS) created within all organization, subordinated to the top management and periodically estimated on certain metrics. The modern science offers various approaches for the solution of this problem; the direction of application risk-focused approach based on system of the international standards (ISO/IEC 27000:2014, 31; ISO/IEC 27001:2013, 23; ISO/IEC 27004:2009, 55; ISO/IEC 27005:2011, 68; ISO/IEC 20000-1:2011, 26; ISO 22301:2012, 24; ISO 50001:2011, 22) is represented as the most perspective.

The economic aspect of IT-security processes, which insufficiently developed as it is observed since the wide range of approaches to a problem of justification of the budget for the set functioning of ISMS. It is noted that directly it is impossible to establish unambiguous dependence between the budget and achievable level of productivity (i.e. ensuring the IT-Security level does not depend obviously only on the size of the allocated funds). Good base submits the annual report of ISO, which contains the statistics considerably expanding opportunities for ISMS modeling, taking into account practice of the previous years, economies of various countries and already known incidents (The ISO Survey of Management System Standard Certifications, 2013).

The management needs the effective instrument of counteraction to modern threats capable to define the most effective decision (to creation of ISMS separately and as a part of the integrated management system (IMS) and to solve the problem defined earlier (Livshitz, 2013; Requirements of the Various Systems of Standardization – ISO 27001 and STO Gazprom, 2015; Podolyanets and Podolyanets, 2011). Counteraction to the corresponding threats at the level of public administration results in need to make political decisions, to enter in particular import substitution programs, which not only the separate enterprises and branches, but also national economy in general.

2. DEFINITION OF A PROBLEM

A number of factors (the considerable cost of the organization assets, the extent of damage from realization of possible threats, the size of excess cost of a complex of IT-security controls) can create a certain risk for economic stability of the organization. Therefore, it is necessary to control a certain balance of these variables, which demands, in turn, effective managing influences. It is expedient in firms to use risk-focused approach that is formulated in a number of international (ISO) and national standards (state standard specifications). The specified approach is based on formation of "context" which consists of external and internal factors. In particular, complex aspects of social and economic conditions in which the organization works are considered.

At creation of the IMS the minimum requirement of the 2nd and more management systems are considered, for example: Quality management system (9000 ISO series), ISMS (27000 ISO/IEC series) and energy management systems (EnMS, 50001 ISO series). In this process, the management can accept as "basic methodology" of IMS various standards containing requirements to safety of business processes in broad economic interpretation of this term. It is known that at creation of modern IMS, besides known problems of cooperation within management systems requirements, it is necessary to provide "integrated compliance" to requirements of business. In terms of "integrated compliance" system effectiveness of safety on criterion function of minimization of expenses and not less significant enclosed task are considered – formal compliance to legislative requirements of various regulators (so-called "compliance," for example, of Russian State Law 63 "Digital sign," Russian State Law 152 "Personal data," Russian State Law 256 "Safety requirements for fuel complex objects"). It is in addition offered to use the ranks of "leaders" of branches presented in work (Requirements of the Various Systems of Standardization – ISO 27001 and STO Gazprom, 2015; Podolyanets and Samoylova, 2013).

Problem definition: Forming the CIF models for assessment based on modern risk-focused standards.

3. REQUIREMENTS OF BUSINESS TO ENSURING THE IT-SECURITY LEVEL

Consider the main requirements of business capable to have considerable impact on the solution of an objective:

1. Requirements of the involved contractors control:
   Modern standards (ISO/IEC 27000:2014, 31; ISO/IEC 27001:2013, 23; ISO/IEC 27004:2009, 55; ISO/IEC 27005:2011, 68; ISO/IEC 20000-1:2011, 26; ISO 22301:2012, 24; ISO 50001:2011, 22) in an explicit form contain requirements to processes of outsourcing, which allow the organizations to carry out more effectively specific processes through authorized intermediaries. Outsourcing of the processes connected with sensitive data can lead to considerable expenses – at a choice of three contractors, costs of infrastructure of data security exceeded on average 1 million US dollars (Livshits et al., 2014; Official web site of "Center for Strategic and International Studies," n.d.; Official web site of "Infosecurity Russia"n.d.; Official web site of Trustwave, n.d.).
2. Requirement of providing 100% of protection:
   At this problem, definition does not demand that for all of assets comprehensive measures (means) of providing IS without exception were introduced. This requirement is submitted logical (in terms of "reasonable behavior of the decision-maker" (Official web site of Trustwave, n.d.) for the organizations which can be carried to CIF. In practice, it is quite enough to receive threshold values of cost of assets and/or the budget, valuable to business, on implementation of measures of providing IB from the decision-maker.
3. Application of organizational measures of IS:
   It is traditionally accepted pertinent not to spend considerable funds for realization of technical systems of providing IS when it is possible to realize organizational measures, for example, within realization of SMIB – as system of management (separately or as a part of ISM).

4. THE ANALYSIS OF THE EXISTING APPROACHES TO A BUDGET ASSESSMENT

The budget on IT-security providing, by different estimates, makes up to 10% of IT budget (in the report [Il'in et al., 2006], budget estimates on IT-security providing are given in range from 3.6% to 3.8% from the IT budget during the period of measurements of 2010-2014). It is characteristic that the maximum value of the IT-security budget makes 6.9% in industrial branch by information for 2014. At the same time, it should be noted that these estimates do not correlate with an assessment of dynamics of growth of incidents number: For example, the average number of the detected IT-security incidents increased in branch of power from 1.179 (2013) to 7.391 (2014), i.e., to 526% (Livshits et al., 2014). Pay attention to statistics of ISMS certification on the ISO 27001 standard on ranks "leaders" (Requirements of the Various Systems of Standardization – ISO 27001 and STO Gazprom, 2015). Research showed that growth of number of the issued ISMS certificates rank from 17% to 22% for "leaders" of the 1st, over 35% for "leaders" of the 2nd rank and from 19% to 27% for "leaders" of the 3rd rank.

5. MODERN RISK-ORIENTED STANDARDS

The risk-focused approach is the main standard for realization the ISO standard series 31000. This standard contains the scheme of a risk management processes which reflects the closed risk management cycle consisting of the main stages – definition of a context, assessment of risk, impact on risk, of monitoring and revision, an exchange of information and consultation (Figure 1). Process of an assessment of risk consists of three consecutive stages – identifications of risk, the analysis of risk and estimation of risk. Preliminary formation of scales for quantitative or qualitative estimation of risks, comparisons of the received estimates to the criteria formed earlier and preparation of the register of risk for processing necessarily is supposed.

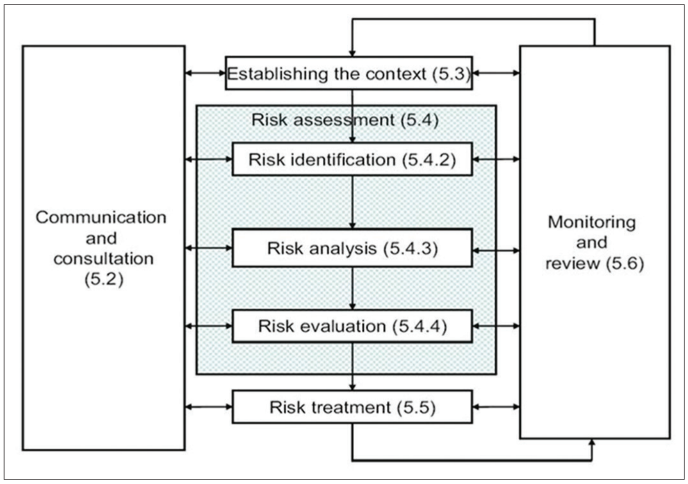
It is known that the term "Risk" (according to item 2.1 of the standard) means "influence of uncertainty on the purposes." Thus in five notes it is specified that influence can be positive and/or negative; the purposes of the organization can have various aspects (for example, financial); the risk is often characterized by the reference to potentially possible events, consequences or their combinations, and uncertainty is the state consisting in insufficiency of information concerning an event, its consequences or its opportunity.

All modern standards (ISO/IEC 27000:2014, 31; ISO/IEC 27001:2013, 23; ISO/IEC 27004:2009, 55; ISO/IEC 27005:2011, 68; ISO/IEC 20000-1:2011, 26; ISO 22301:2012, 24; ISO 50001:2011, 22) are based on risk-oriented approach. The new ISO 9001 standard expected at the end of 2015 also contains the reference to the ISO 31000.

6. PROBLEMS OF A RISK MANAGEMENT FOR CIFS

Management of risk is the process, which is carried out in the organization for the purpose of identification, control, management and control of the events potentially capable to influence achievement of the objectives of the organization. In the offered approach all basic essence are considered: formation of internal and external aspects, a context, system of a risk management and the main types of documentary information – scales of an assessment, criteria of acceptance of risks, the register of risks, the plan of processing of risks and so forth. The example of realization of process of management of risk for the cycle phase "Plan" "Plan-Do-Check-Act" (PDCA) is shown in Figure 2.

Figure 1: Process of a risk management of ISO 31000


Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Communication and consultation (5.2)
Monitoring and review (5.6)

Problems of a risk management for CIF is convenient to arrange as realization of the cycle PDCA (or Deming's cycle):

1. "P" (plan) – Formation of regulatory base, development of regulations, passports of risk, definition of scales of an assessment of risks, criteria of acceptance of risks, forming of summary card of risks for the organization
2. "D" (Do) – Development of actions complex for probability reducing (alleviation of the consequences) at emergence of risks
3. "C" (Check) – Control of completeness, timeliness and efficiency of realization of actions of complex risk management for the organization
4. "A" (Act) – The analysis of productivity of complex of actions risk management at the level of the decision-maker and forming administrative solutions for management system for the organization optimization.

The following important question: End circuit of a cycle PDCA taking into account offered risk-focused approach.

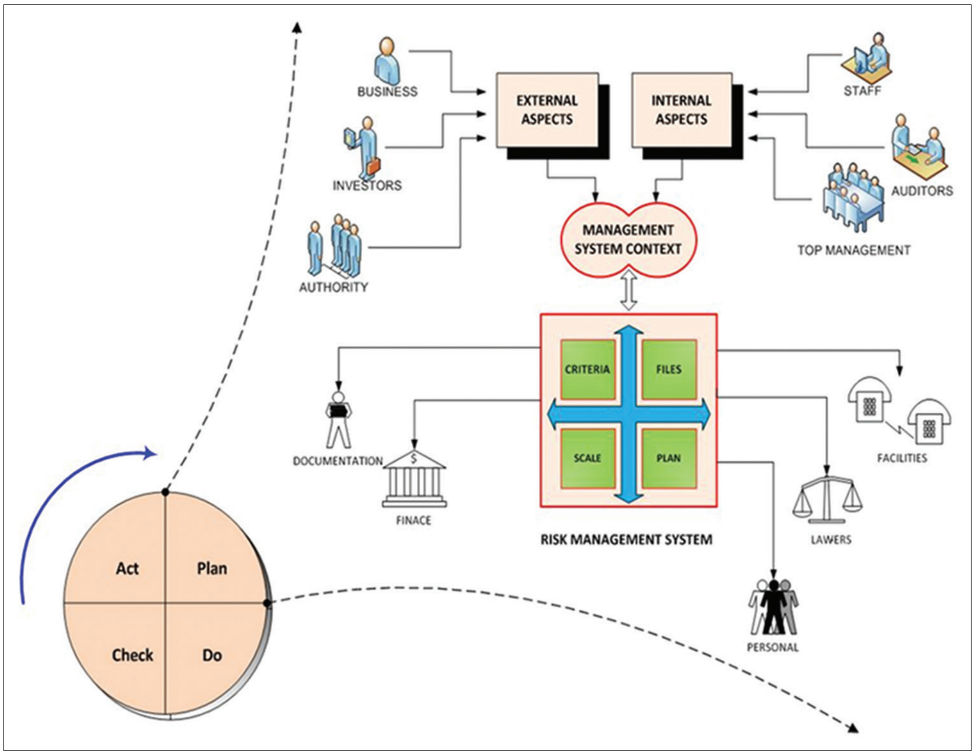
It seems reasonable for CIF to recommend:

- Planning and carrying out internal (including technical) audits – taking into account risk-focused standards (for example ISO 27001 or the new ISO 9001 version).
- Formation of the unified register of discrepancies in the integrated system of management by all types of audits and the analysis of this register from a risk management position (identification of critical points of refusal, the analysis of "cascading" of risks, studying of statistics and so forth)
- Formation of system of expeditious informing the management (for example, based on the standard of management of a business continuity – ISO 22301 or as a part of IMS)
- Accurate distribution of responsibility and powers on each task in the approved program of internal audits, the plan of processing of risks and so forth.

The modern ISO standards rely on uniform risk-focused approach (based on ISO 31000). Respectively, important advantage of all modern systems of management is the requirement of continuous improvement of productivity, which promotes proper response to dynamic changes of a situation, especially manifestations of actual threats for CIF:

- Increase in number of leakages of sensitive information (commercial, technical, financial, personal);
- Strengthening of critical consequences of loss of assets, valuable to business;
- Strengthening of degree of consequences of blocking of work of critical systems (financial, transaction, logistic, information and so forth);
- Impossibility of fast replacement, repair or purchase of new expensive import equipment (technologies) or accessories.

Figure 2: Process of management of risks for the cycle Plan-Do-Check-Act phase "Plan"



7. MODEL OF FORMATION OF A VALUE ADDED IN SYSTEMS OF MANAGEMENT

The management forms the business purposes of the organization proceeding from a wide set of entrance factors impact on which have various interested parties. In the presented model the main interested parties – competitors and regulating boards, which total influence makes the dominating impact on any organization (Figure 3). After formation of the business purposes business processes in the organization are built (it belongs also to processes of an outsourcing and/or outstaffing equally). One of the purposes of formation of system of business processes is definition of requirements to resources (for example, involvement of the third-party personnel possessing rare qualification).

The following stage concerns the accounting of assets of the organization (in relation to CIF it is correct to tell about various categories of the equipment, means of communication, licenses for the software, the personnel, etc.). On this stage metrics of an assessment of effective use of assets of the organization have to be offered and coordinated. At the following stage determination of productivity of business processes of the organization on the basis of the coordinated metrics because of operating process is possible only on the basis of reliable estimates, factual (ISO/IEC 27001:2013, 23).

In end of a cycle, it is necessary to execute an assessment of productivity of business processes of the organization and to make the adequate administrative decision – is it enough to carry out routine procedure of continuous improvement, without essential changes, or cardinal actions for optimization of activity of the organization are necessary.

8. MATHEMATICAL PROVISION FOR CIFS AUDITS

We made definition of introduced unilaterally limit (more precisely, the limit of a function on the left). The number of A ∈ R is called the left limit of function *f (x)* at the point "a," if for any positive number ε will be found corresponding to his positive number δ, such that for all x in the interval (a - δ, a) the inequality (Nogin, 2007; Il'in et al., 2006):

$$| f(x) - A | < \varepsilon$$

or

$$\lim_{x \to \alpha - 0} f\left(x\right) = A \Leftrightarrow \forall\, \varepsilon > 0 \exists \delta$$

$$= \delta\left(\varepsilon\right) > 0 \forall x \in \left(\alpha - \delta,\ a\right) : \left| f\left(x\right) - A \right| < \varepsilon$$

The derivative of the function *f (x):*

$$lim_{\ \Delta x \to 0} = \frac{f\left(x + \Delta x\right) - f\left(x\right)}{\Delta x} = \lim \frac{d}{dx} f\left(x\right) = f^{'}\left(x\right)$$

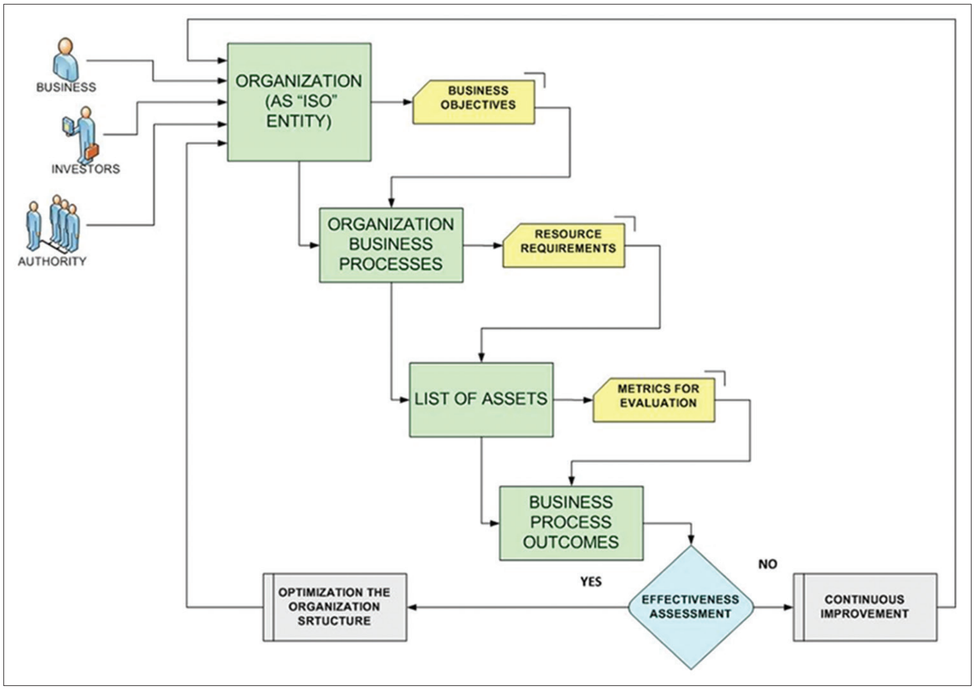
The corresponding one-sided limit is called the derivative of the left-designate $f'(x)$.

An example of partial derivatives definition for instantaneous IT-security audits:

The left derivative allows to estimate the desired interval, which can be changed if necessary in the ISMS and reasonable conduct a new IT-security audit. Consider the real function of variables:

$y = f(x_1, x_2, x_3, \ldots, x_n)$

Figure 3: Formation of a value added in the integrated management system model of the organization



Where, for example, the first four variables describe attributes for IT-security audits:

x_1 – Frequency of audits, defined as the ratio of audits number for the ISMS in the observed period;

x_2 – The scope of the audit program, defined as the ratio of the processes number covered by the total count of processes in the stated certification scope of the ISMS;

x_3 – Metric achieve the level of protection which is defined as a measure of the effectiveness of the ISMS *Rbase*/*Rmax*;

x_4 – Metric corrective actions planned for the range of IT-security audits.

Then the partial derivative of the first order by the first variable x_1 is:

$$\lim_{\Delta x_1 \to 0} = \frac{f\left(x_1 + \Delta x_1, x_2, x_3, \ldots, x_k\right) - f\left(x_1, x_2, x_3, \ldots, x_k\right)}{\Delta x_1}$$

$$= \frac{\partial}{\partial x_1} f(x)$$

The partial derivative:

$$\frac{\partial y}{\partial x_1} = f\ 'x_1\left(x_1, x_2, x_3, \ldots, x_n\right)$$

At each point (x_1, x_2, x_3,…,x_n) is a measure of the rate of change of y with respect to x_1 as fixed value of the remaining independent variables. All the partial derivatives can be found by differentiating $f(x_1, x_2, x_3, \ldots, x_n)$, for x_n, if the other $n-1$ independent variables are considered as constant parameters. If $y = f(x_1, x_2, x_3, \ldots, x_n)$ has at the point (x_1, x_2, x_3,…,x_n) all continuous partial derivatives of the first order, it is at this point the first differential:

$$dy = \frac{\partial f}{\partial x_1} dx_1 + \frac{\partial f}{\partial x_2} dx_2 + \ldots + \frac{\partial f}{\partial x_n} dx_n$$

For one changed variable x_1 (for example, the frequency of IT-security audits) will evaluate the practical value of the partial derivative (at constant other variables), we estimate the growth rate of the ISMS security level:

$$\frac{\partial}{\partial x_1} = f\ 'x_1\left(x_1, x_2, x_3, \ldots, x_n\right) = \frac{\Delta R_k}{\Delta\ t\ k}$$

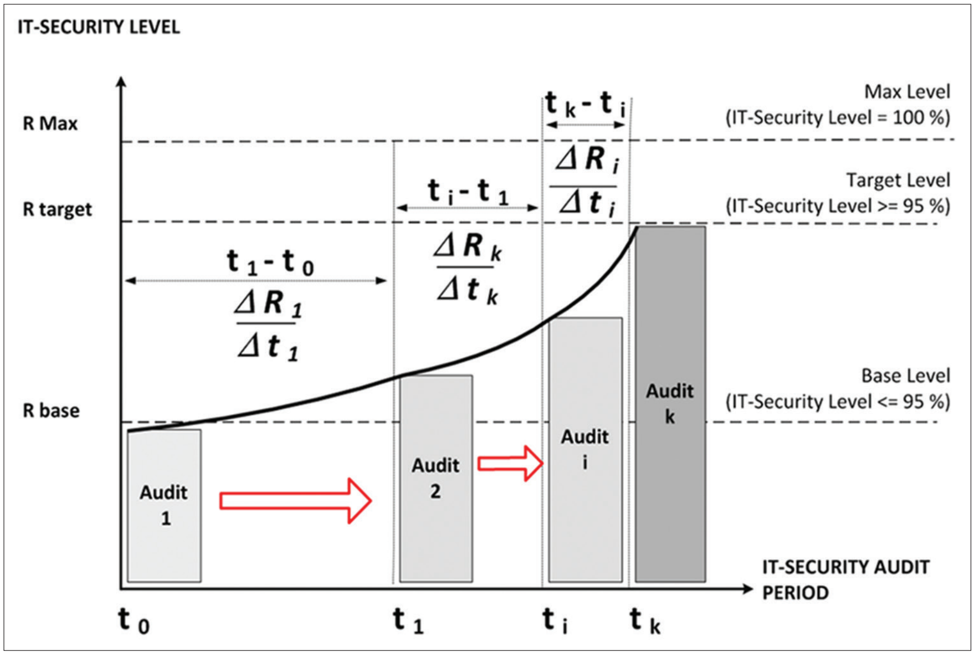
The solution of the problem can be shown as a reduction of the period of IT-security audits in complex industrial object when using the left function variables. For example of one variable x_1 demonstrated an increase in the growth rate of the protection level for known $\frac{\Delta R_k}{\Delta t\ k}$ variables ISMS audit process (Figure 4).

9. COMPREHENSIVE AUDIT OF COMPLEX INDUSTRIAL OBJECT IN THE MANAGEMENT SYSTEM

The ISO standard 19011 indicates that the audit objectives can be formed on the basis of the requirements for the estimation:

- The level of activity of the audited facility, reflecting the degree of repeatability non-conformance or incidents;
- Consequences that have occurred internal and/or external accidents;
- Performance management systems in relation to its objectives;
- The effectuation to legal, legislative, contractual requirements in the management system ("compliance");
- Similar results obtained at other sites that help identify trends.

Figure 4: Example of increase in growth rate of level of IT-security on one variable



In a set of international standards (ISO/IEC 27001:2013, 23; ISO 22301:2012, 24) several approaches to assessing the effectiveness and efficiency of business processes are proposed, but a unified system of loss assessment (of categorization) is not represented. Based on the practice of audits performed authors proposed the following structure of categories to determine the numerical value of the loss:

- Extra time (e.g. redundant requests and coordination);
- Extra people (e.g. employees, creating a complex chain of coordination and so on);
- Extra resources (e.g. disordered version of the software);
- Unnecessary actions (such as non-consensual deployment of IT-systems).

As an example, showing the importance of taking into account the requirements in order to ensure a comprehensive IT-security provides about breach a control systems of industrial safety of the hundreds of European and American energy companies malware (such data are given in the report of the company Symantec, link - http://hitech.newsru.com/article/01jul2014/dragonfly). According to Symantec, hackers used malware EnergeticBear, which allows to monitor energy consumption in real time or damaging physical systems (including turbines, gas pipelines and power plants). This program is similar to the virus Stuxnet, which was used to infect Iran's uranium enrichment facilities. Experts believe that hacker used EnergeticBear for 18 months for attacks on computer systems by more than 1000 organizations in 84 countries.

10. FORMATION OF THE LIST OF PROTECTED ASSETS FOR COMPLEX INDUSTRIAL ENERGY FACILITIES

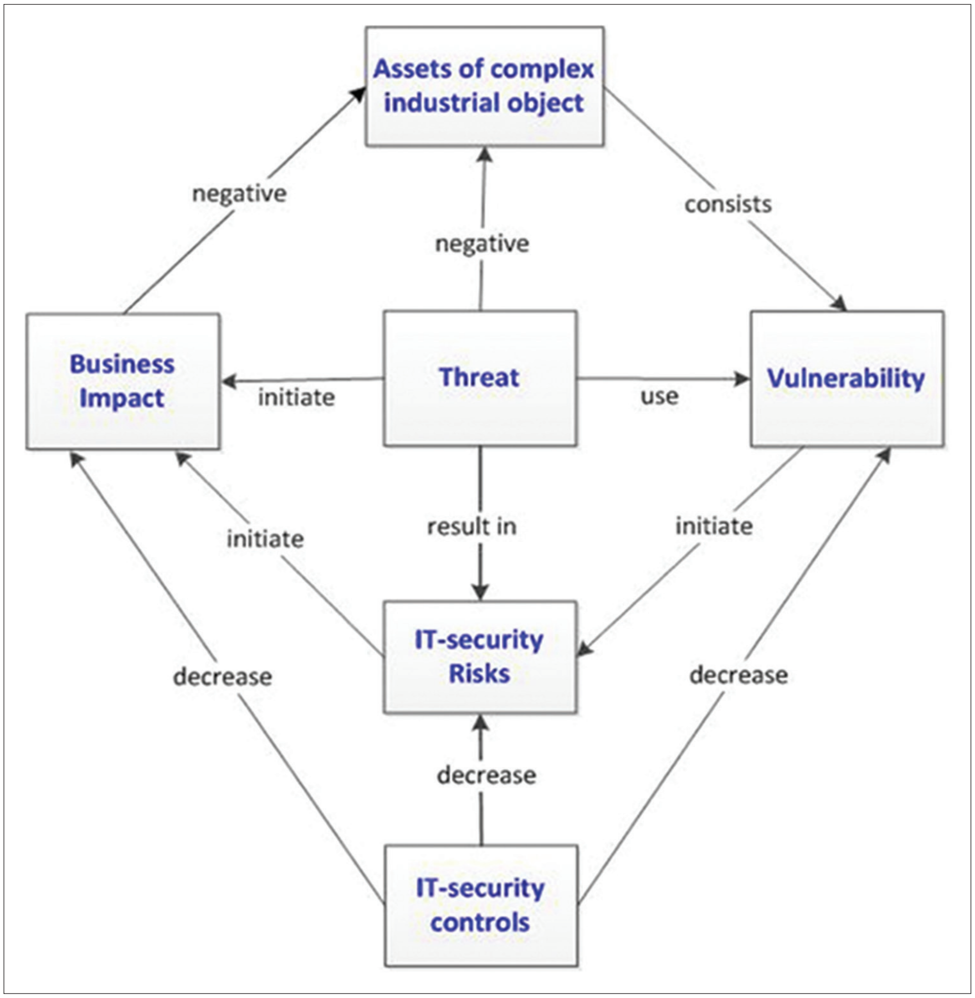
In any management system (Livshitz, 2014), the first and one of the most important issues is the correct identification of the list of assets that require protection against acts of unlawful interference. For energy problem identification and protection of "critical facilities" (in the terminology of Federal law of Russian Federation 256-FZ 2011, July 21 may be compared with the general problem of identifying and protecting valuable business assets in ISMS/or IMS. The approach to the identification and valuation of assets for the ISMS can be represented (Figure 5). Note that properly defined and categorized assets "are the key" to the correct formation of possible threats list in the current notation of documents from the Russian Federal Service of Technical and Expert Control (FSTEC) and, accordingly, a realistic assessment of possible damage to energy complex industrial object.

On the basis of the generated list of assets to be protected, the next step is determined by the list of vulnerabilities and threats. To counteract (decrease) certain measures to ensure IT-security (in the notation of ISO [ISO/IEC 27000:2014, 31] control) are being applied. The ultimate goal of application of IT-security measures is to reduce the potential damage in respect of chosen assets of energy complex industrial object. Accordingly, it is assumed that the list of assets to be protected, is in a certain balance with respect to the cost of IT-security controls, providing economic efficiency ISMS principle. It is recommended to use conjunction Appendix "B" standard ISO (ISO/IEC 27005:2011, 68) and FSTEC regulations to generate the list of threats. The criteria used as the basis for assigning values to each asset in the organization of Energy, should be clearly defined: The original value, the cost of replacement (reconstruction) of the asset in case of the worst-case scenario act of unlawful interference (IT-security risk events), or added value (for example, the value of reputation) (ISO/IEC 27001:2013, 23; ISO/IEC 20000-1:2011, 26; ISO 22301:2012, 24).

11. THE BASE MODEL FOR THE IMS AUDITS

The IMS model contains all the basic content for performing audits (criteria, evidence, object surveillance audit). It allows to create assess

Figure 5: Interaction of concepts IT-security management system



the IT-security level (Livshitz, 2013). The audit process provides an important component of the overall (integrated) assessing the IMS effectiveness. It allows to efficiently perform the decomposition of "general" objectives in the IMS specific objectives, such as assessing the IT-security level. Figure 6 is a basic model for ISM audits.

General explanations of the basic model of IMS are:

- ISM audit involves the use of a single set of metrics on the functioning of different interfaces for internal audits and external audits;
- Internal audits required to take into results of the external audits; converse is also true;
- The impact on the assessment of the object is realized through the management review subsystem (in accordance with the PDCA cycle).

12. THE IMS MODEL FOR CONDUCTING AUDITS IN THE AIRPORT COMPLEX (ACS)

The requirements (basic and advanced) refer to the AC, which can be considered fully complex industrial object. Firstly, they require strict compliance with regulatory requirements of the AC and, secondly, they require periodic inspection performed of the AC specific requirements (Livshitz, 2014). In the aspect of the ISM requirements for audits practical question of the superiority of any criterion (standard requirements, regulations, etc.) opposite the other is relevant. Accordingly, a task is advisable to decide on the basis of the model ISM audits, supplemented with a special power optimization - for the safety assessment (Figure 7). Given these characteristics of the comprehensive audit of AC, the central focus should be on the optimization block in the IMS AC model.

The unit allows for optimization at the entrance level of efficiency of business processes and AC fulfills the necessary changes in the model of the IMS output. It allows to make control actions via the optimization of feedback channels from the basic model complex industrial object IMS - through the assessment of the effectiveness (the extent to metrics) and the periodic review of IMS by management. This object is achieved through the performance evaluation for individual functional subsystems ISMS or IMS.

13. THE IMS MODELS FOR CARRYING OUT AUDITS IN THE ENERGY SECTOR

Formation of the list of threats, model of the violators and the threat model must be based on known and practically spent database vulnerabilities, differentiated according to specified parameters. It is useful to review the list of typical threats and

Figure 6: Basic model of integrated management system audits

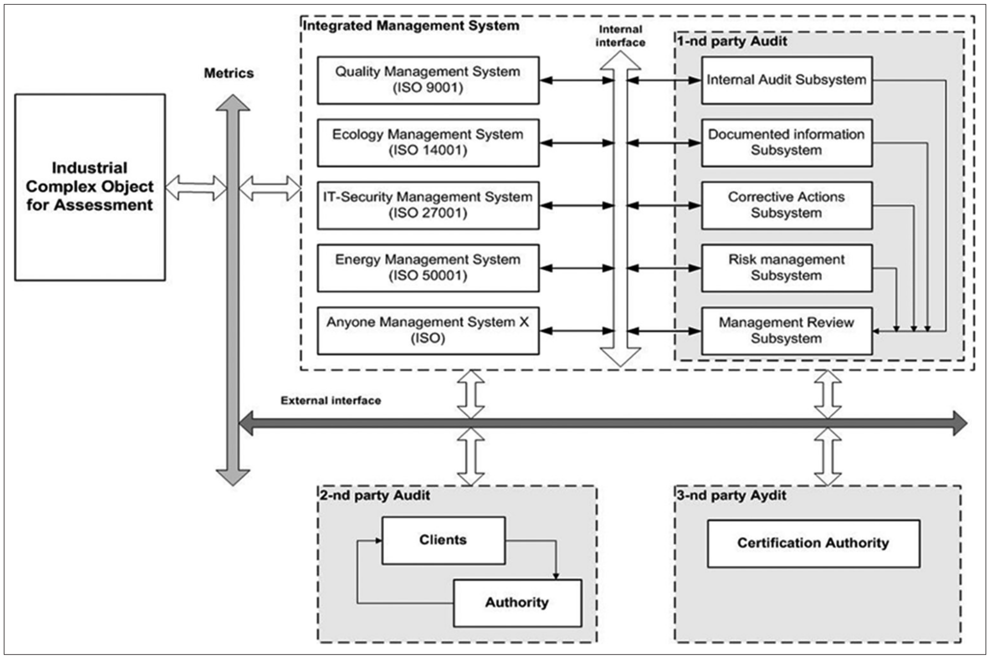
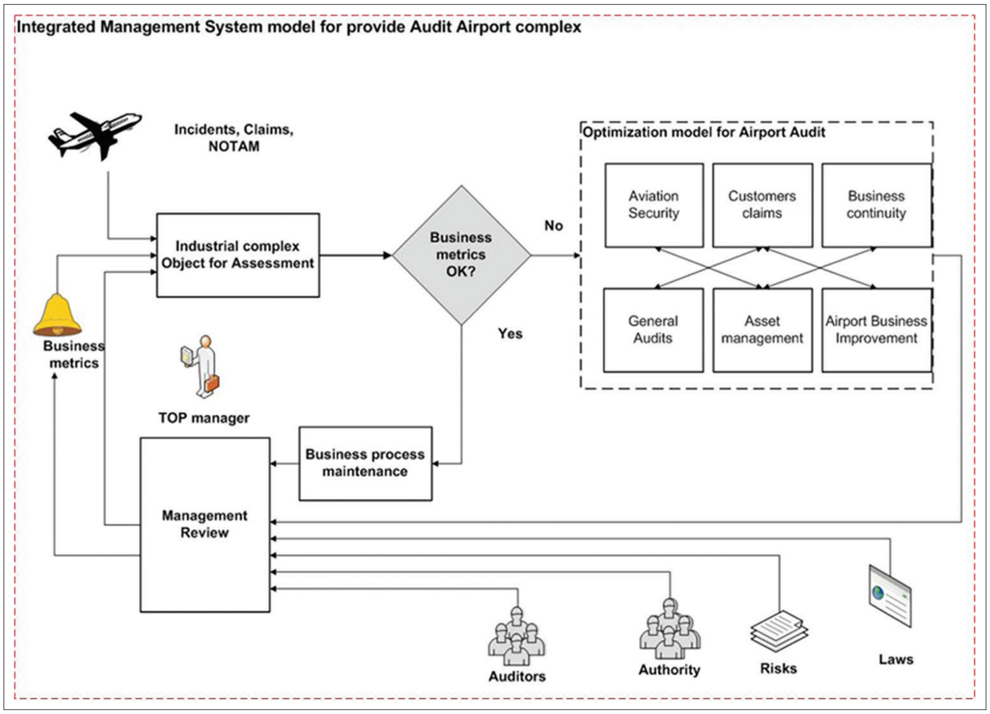

Integrated Management System
Internal interface
1-nd party Audit
Metrics
Quality Management System (ISO 9001)
Internal Audit Subsystem
Ecology Management System (ISO 14001)
Documented information Subsystem
Industrial Complex Object for Assessment
IT-Security Management System (ISO 27001)
Corrective Actions Subsystem
Energy Management System (ISO 50001)
Risk management Subsystem
Anyone Management System X (ISO)
Management Review Subsystem
External interface
2-nd party Audit
Clients
Authority
3-nd party Aydit
Certification Authority

Figure 7: The IT-security management systems model for audit of airport complex



vulnerabilities in accordance with Annex "D" 27005 Standard (ISO/IEC 27005:2011, 68) (Table 1).

Based on the example of threats and vulnerabilities, the following model for the purpose of ISM Audit for complex industrial object in the energy sector is offered (Figure 8):

Example of the ISMS effectiveness calculation:

Consider the calculation IMS model that takes into account the key variables that allows to create conditions to reduce the risk of valuable assets of complex industrial object:

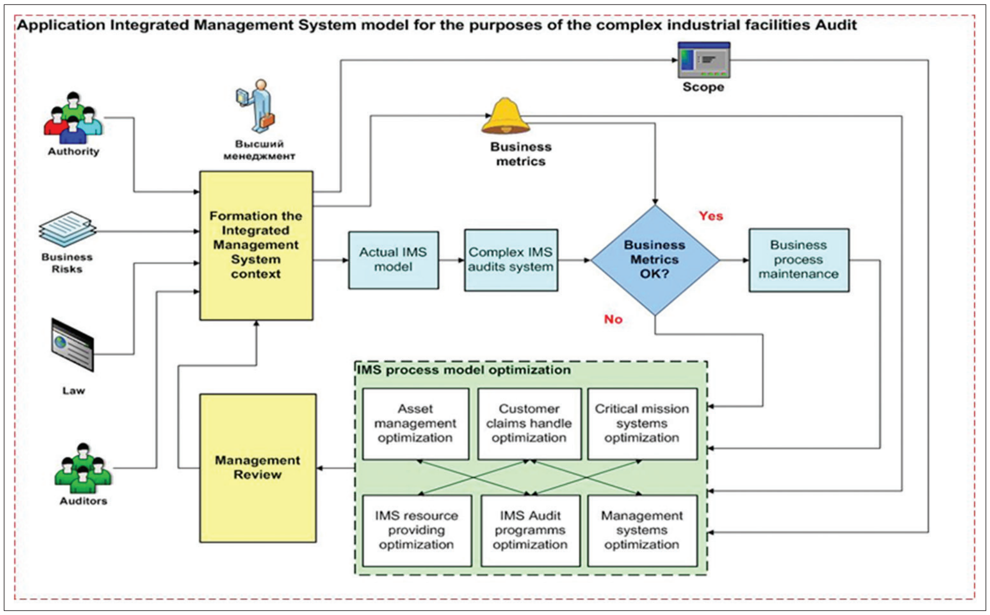
- C_{asset} – The value of protected assets;
- $C_{incident}$ – The cost of the damage caused by the implementation of possible incidents;
- P_{IMS} – The level of management system (IMS) performance;
- $C_{control}$ - The value of the security tools complex ("controls").

The proposed model for the ISM audits of complex industrial object considers numerical metrics that allow to vary parameters: C_{asset} = 1,000,000 RUR, $C_{incident}$ = 180,000 RUR, P_{IMS} and 4 values (depending on results of all types of ISM audits (internal and external) – 0.5, 0.7, 0.9 and 0.99). Suppose that the number of

Table 1: Vulnerability and vulnerability assessment methods

Type	Vulnerability	Threat
Hardware	Susceptibility to voltage variations	Loss of power supply
	Unprotected storage	Theft of media or documents
Software	No or insufficient software testing	Abuse of rights
	Lack of audit trail	Abuse of rights
Network	Poor password management	Abuse of rights
	Lack of effective change control	Software malfunction
	Lack of physical protection of the building, doors and windows	Theft of media or documents
Personal	Absence of personnel	Breach of personnel availability
	Inadequate recruitment procedures	Destruction of equipment or media
Object	Unsupervised work by outside or cleaning staff	Theft of media or documents
	Lack of procedures of risk identification and assessment	Abuse of rights
	Lack of continuity plans	Equipment failure
	Lack of control of off-premise assets	Theft of equipment

Figure 8: The IT-security management systems model for audit of energy industry


Application Integrated Management System model for the purposes of the complex industrial facilities Audit
Scope
Authority
Высший менеджмент
Business metrics
Business Risks
Formation the Integrated Management System context
Actual IMS model
Complex IMS audits system
Business Metrics OK?
Yes
No
Business process maintenance
Law
IMS process model optimization
Asset management optimization
Customer claims handle optimization
Critical mission systems optimization
Management Review
Auditors
IMS resource providing optimization
IMS Audit programms optimization
Management systems optimization

IT-security incidents ($N_{IT\text{-}security}$) that could harm the assets of the organization is growing unevenly throughout the year (according to the law, nearly exponential), and, at some point, without adequate actions, be comparable to the cost of the organization's assets, and completely destroy the business. Consider the example of countering the negative factors $C_{incident}$ for the IMS: 8 months, the size of the potential damage from IT-security incidents will be $C_{incident}$ = 420,000 RUR (right scale), which already exceeds the cost of implement a set of safety equipment $C_{control}$ = 180,000 RUR, and the degree of effectiveness of the IT-security system P_{IMS} was determined to be 0.7. Example of calculating the ISMS efficiency is shown in Figure 9. Left scale shows the valuation of assets, security controls and the resulting data for the ISM. Right scale separately shows rising costs of IT-security incidents that can adversely affect the organization assets. In this example, the actual value of organization assets A_{ISM} (due to realized complex of IT-security controls) will be:

$$A_{ISM} = C_{asset} - C_{control} - C_{incident}*(1 - \text{PIMS}) = 1{,}000.000 - 180.000 - 420.000*0.3 = 694.000 \text{ RUR}$$

$$dy = \frac{\partial f}{\partial x_1}dx_1 + \frac{\partial f}{\partial x_2}dx_2 + \ldots + \frac{\partial f}{\partial x_n}dx_n$$

Note that without the implementation of IT-security controls the assets cost A_{ISM} under $C_{control}$ = 0, and the same amount of $C_{incident}$ will be:

$$A_{ISM} = C_{asset} - C_{incident} = 1{,}000.000 - 420.000 = 580.000 \text{ RUR}$$

With increasing of the IMS time positive experience in combating the negative effects of the $C_{incident}$ on the valuable assets of the organization will accumulate, which ultimately increases the ISMS effectiveness and the overall stability of the business (Figure 10). Note that the reduction of $N_{IT\text{-}security}$ increases objectively assessment the performance of the ISMS P_{IMS}, as a factor in reducing the impact (Livshitz, 2014).

14. CONCLUSIONS

1. Refined security model of complex industrial object on the basis of a risk-based approach both for the energy complex and airport; while noting the importance of the "closing" principle of PDCA cycle in the creation and evaluation of management systems;

Figure 9: Assessment of economic efficiency of IT-security management systems

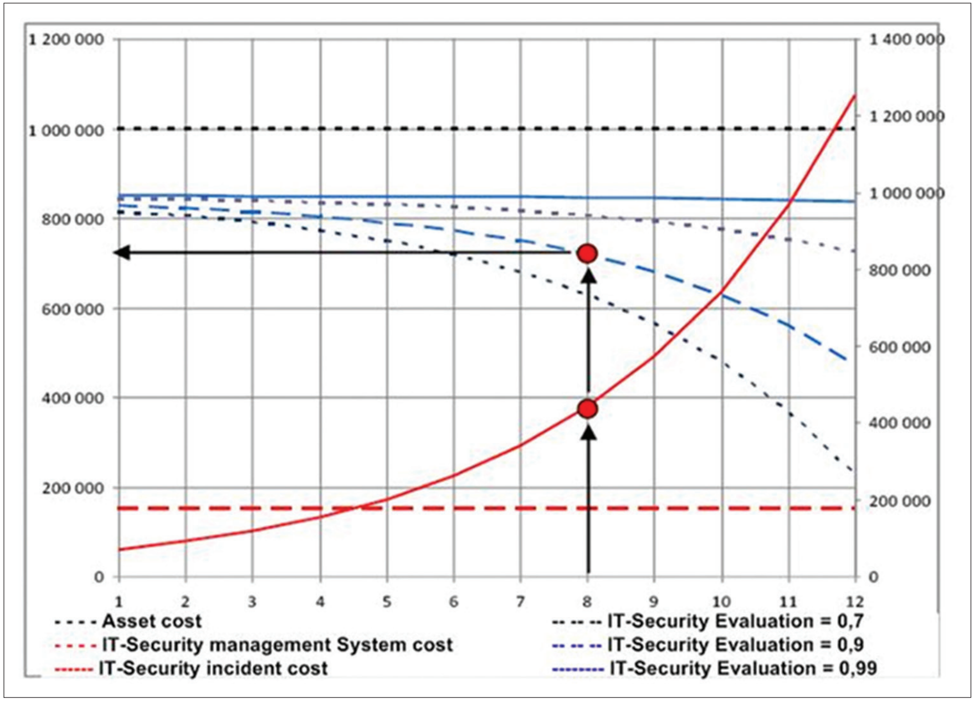
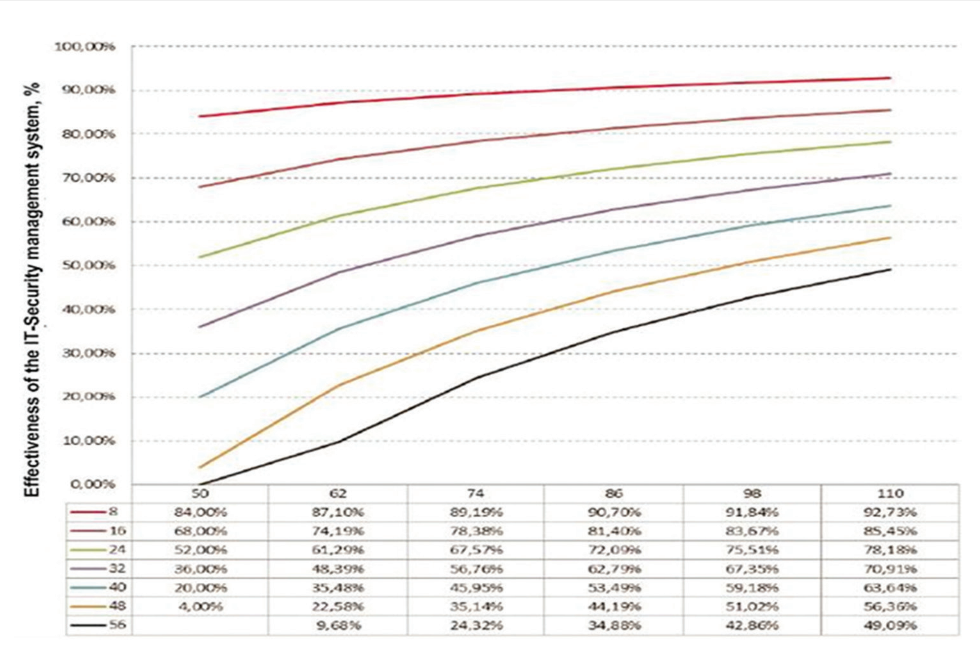


Figure 10: Calculation of productivity of IT-security management system



	50	62	74	86	98	110
8	84,00%	87,10%	89,19%	90,70%	91,84%	92,73%
16	68,00%	74,19%	78,38%	81,40%	83,67%	85,45%
24	52,00%	61,29%	67,57%	72,09%	75,51%	78,18%
32	36,00%	48,39%	56,76%	62,79%	67,35%	70,91%
40	20,00%	35,48%	45,95%	53,49%	59,18%	63,64%
48	4,00%	22,58%	35,14%	44,19%	51,02%	56,36%
56		9,68%	24,32%	34,88%	42,86%	49,09%

2. An approach that allows to use in assessing the management systems of complex industrial object reduces the period of conception of IT-security audits. This increases the speed of audits process conducting, management responses and increases growth of IT-security protection level;
3. It is shown that the ultimate goal of applying set of IT-security controls is ensurement that reduce of potential damage in respect of selected assets of complex industrial object. Accordingly, balance of the cost of the IT-security controls and the total cost of the protected assets is provided, which, in turn, provides the principle of economic efficiency.

REFERENCES

Federal Law of the Russian Federation #256-FZ, "About safety of objects of fuel and energy complex", Rossijskaja gazeta [Russian newspaper] July 26, 2011, No. 161.

Il'in, V., Sadovnichi, V., Sendov. B. (2006), Theory of limit. Mathematical Analysis. Vol. 1. Ch. 3. Moscow: Prospect. p672. (In Russia).

ISO 22301. (2012), Societal Security – Business Continuity Management Systems – Requirements. Geneva: International Organization for Standardization.

ISO 50001. (2011), Energy Management Systems – Requirements with Guidance for Use. Geneva: International Organization for Standardization.

ISO/IEC 20000-1. (2011), Information Technology – Service Management - Part 1: Service Management System Requirements. Geneva: International Organization for Standardization.

ISO/IEC 27000. (2014), Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. Geneva: International Organization for Standardization.

ISO/IEC 27001. (2013), Information Technology – Security Techniques – Information Security Management Systems – Requirements. Geneva: International Organization for Standardization.

ISO/IEC 27004. (2009), Information Technology – Security Techniques – Information Security Management – Measurement. Geneva, Switzerland: International Organization for Standardization.

ISO/IEC 27005. (2011), Information Technology – Security Techniques – Information Security Risk Management. Geneva: International Organization for Standardization.

Livshits, I., Moldovyan, A., Tanatarov, A. (2014), Study of certification dependency of international standards ISO types from the organization for leading industries. Proceedings of SPIIRAS, 3(34), 160-177. (In Russia).

Livshitz, I. (2013), Joint problem solving information security audit and ensure the availability of information systems based on the requirements of international standards BSI/ISO M. Informatisatia i Svyaz', 6, 62-67. (In Russia).

Livshitz, I. (2014), Approaches to the application of the integrated management system model for carrying out audits for complex industrial facilities – Airport complexes. Trudy SPIIRAN, 6, 72-94. (In Russia).

Livshits.I (2015) Requirements of the Standardization Systems – ISO 27001 and STO Gazprom, Proceedings of SPIIRAS, 3, 33-44.

Nogin, V.D. (2007), Decision Making with Multiple Objectives. Saint-Petersburg: State University – Higher School of Economics. p103.

Official web site of "Center for Strategic and International Studies". (n.d.), Available from: http://www.csis.org. [Last accessed on 2015 Jul 07].

Official Web Site of "Infosecurity Russia". (n.d.), Available from: http://www.infosecurityrussia.ru. [Last accessed on 2015 Jul 07]. (In Russia).

Official Web Site of Trustwave". (n.d.), Available from: http://www.trustwave.com. [Last accessed on 2015 Jul 07].

Podolyanets, L.A., Podolyanets, D.V. (2011), Algorithmization of creation of corporate information systems (CIS) at the industrial enterprises. Economy. Taxes. Right. Moscow: Federal State Educational Budgetary Institution of Higher Professional Education "Financial University Under the Government of the Russian Federation". p2.

Podolyanets, L.A., Samoylova, L.K. (2013), Financial control as element of system of economic security of the state. News of the Orenburg state agricultural university. Orenburg state agricultural university. Orenburg, 3(41), p.197-201.

Ryabinin, I.A. (2007), Reliability and Safety of Structurally Complex Systems. St. Petersburg: St. Petersburg State University. p276.

Solozhentsev, E.D. (2011), The WTO and the logical-probabilistic models of non-validity of complex systems and processes. Journal of Economic Theory, 4, 136-147.

Solozhentsev, E.D. (2014), Technologies of logic and probabilistic management of risk of social and economical systems. International Journal of Risk Assessment and Management (IJ RAM), 17(3), 171-187.

Official Web Site of ISO (2014), the ISO Survey of Management, System Standard Certifications, Available from: http:// www.iaf.nu/articles/ISO_Survey_2014/449.