The Method of Implementation of the Numerical IT-Security Metrics in Management Systems

Ilya Livshitz
ITMO University
St. Petersburg, Russia
livshitz.il@yandex.ru

Pavel Lontsikh, Sergey Eliseev
Irkutsk National Research Technical University
Irkutsk, Russia
palon@list.ru, eliseev_@inbox.ru

***Abstract*—The relevance of the publication is called by the attention to the problem of formation of reliable measurement results (estimates) of the IT-Security management systems' (ISMS) effectiveness. Decision-makers must operate reliable results of carrying out the measurements of ISMS based on objective quantitative metrics of IT-Security. Known methods for evaluation of the safety systems are presented excluding the PDCA cycle requirements and apart from the general requirements directly to the ISMS. The study of the applicable standards (ISO, NIST, and GOST) and the current practice allowed us to propose an approach to the explanation of a technique of formation of IT-Security metrics, that numerically let us to assess the effectiveness of the ISMS. The results can find a practical application in the independent efficiency evaluation of the ISMS.**

I. Introduction

In modern scientific papers on the subject of safety assessment [1 - 4] are considered some aspects of the selection of IT-Security metrics and application of effectiveness indicators of information processes (including assessment for IT SOX requirements). Processes of evaluation of the Integrated management systems (IMS) are presented without taking into account the requirements of PDCA cycle, and apart from the general requirements, which are presented, in particular, to the information security management systems (ISMS). This current situation does not fully correspond each of the requirements of a modern risk-based standards ISO and existing threats to IT-Security, and forms the background for the need to solve the problem of measurement and numerical evaluation of the effectiveness of the ISMS.

In the present study we assume the object of the ISMS, which is an open system that constantly implements secure exchange (in particular - information) with the external environment. The ISMS is created for an effective response to external negative influences of the environment on the protected system [1], [7]. These effects can be described in the parameter space (in practice - information security metrics), in which the observer – the decision maker objectively judges the status of the protection system in the required time.

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). 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).

II. Statement of the problem

It is proposed to solve the above problems to apply standards ISO 27000 [17 - 20] as normative base, and also NIST 800-53 series of recommendations [21], completed by specially optimized theory "elite groups" for the PDCA cycle. It should be noted that not all experts uniquely precise understand the essential difference in terminology: "effectiveness" is different from the "efficiency" [17]. Accordingly, metrics differ, applied by information security experts in the measurements of the effectiveness of the ISMS, that hinders the formation of decision-makers' objective recommendations for planning and implementation of the necessary program measurements. At the same time the success of the series 27001 standards attracted the attention of experts (see. Date overview of the ISO 2014 [22]), and contributes to the unification of applied techniques measurements and the formation of a set of information security metrics based on the ISO [19].

It is necessary to define the relevant stake holders [14], which should be involved in determining the scope of the ISMS measurement. Specific results of effectiveness tools measures of information security ensuring should be defined (controls [14]) and brought to the attention of stake holders, which may be internal or external to the organization (paragraph 7.2 of the standard [14]). Accordingly, we need a control mechanism of transferring data for different interfaces, such a model system is presented in the publication [19]. Information security metrics system can support the making decision of decision-makers at the appropriate levels of the hierarchy of the ISMS, for example, determining the effectiveness of the main activities that depend on providing a given level of information security decision-makers [9], [11].

In view of the above statement, the problem is formulated as follows: the development of methods of forming the numerical (quantitative) information security metrics to assess

the effectiveness of the ISMS, which are relevant to hierarchical control system of organization.

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.

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/IEC 27000:2014 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) 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 series 27001, ISO/IEC series 20000-1, ISO series 22301).

III. Identified contradictions

The study of mentioned above papers and regulatory framework revealed the following contradictions:

1) The first contradiction is due to the fact that a significant number of developed standards (international, state, industry) determines the widest variation of combinations of their use to ensure information security objectives. In particular, a number of national standards GOST R "do not have time to" be updated simultaneously with the revision of ISO standards (e.g., ISO/IEC series 27001 and GOST R ISO/IEC 27001).
2) The second contradiction is determined by the fact that the selection of the best sets of applicable metrics of information security for ISMS assessment on the criterion of best achieving of the goal, in particular the ensuring of the specified level of information security, is hindered with the lack of a single guaranteed "reasonable approach" of decision-makers mechanism (in terms of Pareto). Accordingly, there are the following critical risks:

- the incorrect definition (immeasurable) of the creation purposes of the ISMS as hierarchical management system of complex object;
- the technical solutions are not fully able to provide the required level of information security software for a given list of business processes.

IV. Basic requirements to the procedure of formation of information security metrics

In the aspect of formulation of the problem it is important that the standard [14] defines the requirements for the measurement program (paragraph 5.2.), in particular - to provide the measurement results to interested parties to determine the need for improvement of the ISMS. These requirements are, in fact, represent a clear "mini-cycle" of the PDCA, which is implemented in the ISMS on the respective hierarchical levels of management system and "supplies" the decision-makers with the data to make effective management decisions. Methods of selecting the specific metrics of information security should focus on the quantitative measurement of ensuring information security in relation to the protected assets [12], [19].

At the same time in a number of publications [1 - 8] and normative documents are not shown the necessary information security metrics (even the simplest), on the basis of which you can create the system of effectiveness measurement of ISMS. In particular, GOST [20] for the protection of the media are just a few of vitality indicators: operating temperature range, the operating range of relative humidity (see Table 1 and 2 in [21]). Table. 9 standard [20] shows the nomenclature of quality indicators, which can be supplemented from the "C" application [16] in terms of vulnerabilities, such as: "Vulnerability Assessment" (paragraph 1.2.7. [15]). Thus, the proposed method of forming IT-Security metrics for measuring the effectiveness of the ISMS create based on the ISO 27001 series and other regulatory documents (GOST, the NIST), as well as optimized the theory of "elite groups" [22]), allowing to obtain reliable and reproducible evaluation.

Accordingly, it can be offered to different categories of information security metrics aligned to the type of the protected assets of organizations, such as: simple metrics; complex metrics; combined metrics. The criteria for division of IT-Security metrics on the above categories are invited to use the following rules:

- simple metrics can be obtained directly by specialists IT-Security service through technical means or by the results of the analysis of information security measures (for example, when analyzing the "logs" firewalls, SIEM systems, reports the results of audits of IT-Security, etc.);
- complex metrics are calculated based on simple metrics and require the use of additional services other specialists (for example, the valuation of the protected assets requires data from the financial and economic units);

- combined metrics are calculated on the basis of complex metrics and require the involvement of senior management responsible for the safe execution of certain business processes. Moreover, given the direct relevance of complex metrics to protect the assets and evaluation, including damages for the calculation of this category IT-Security metrics should be allowed a limited number of managers.

V. Requirements for selection of measurement method

For each measurement of the main action must be determined by the method of measurement, which is used for the quantitative determination of the measurement object by giving the attribute values attached to the main measurement as [15]. It is recommended to apply an objective measuring method, which uses a quantitative assessment, which may be implemented "machine" means (IPS, SEIM, DLP). Importantly, in terms of FZ-102 is specified class of such funds' technical systems and devices with measuring functions - technical systems and devices, which in addition to their basic functions operate measurement functions". This suggests the application - just for a practical purpose receive automatic "machine" data to form an overall quantification of the level of IT-Security.

For each measurement method should be established and documented verification process that ensures the trust level to a value that is achieved by using a measurement method for measuring an attribute of the object and is assigned to the main measurement measures. The method of measurement must remain uniform over "operational" time (as in a "mini-cycle" PDCA, and full cycle PDCA ISMS), so that the emphasis placed on the main (derivative) measurement measures and received at different times, were comparable [15], [16].

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.

On the basis of the generated list of assets to be protected, the next step is determined by the list of vulnerabilities and threats. 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 Appendix “B” standard ISO (ISO/IEC 27005:2011). 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 series 27001).

VI. The analysis of the existing approaches to assessment

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 vulnerabilities in accordance with Annex “D” 27005 Standard (ISO/IEC 27005:2011). Based on the example of threats and vulnerabilities, the following model for the purpose of ISM Audit for CIFs in the energy sector is offered (see Fig. 1):

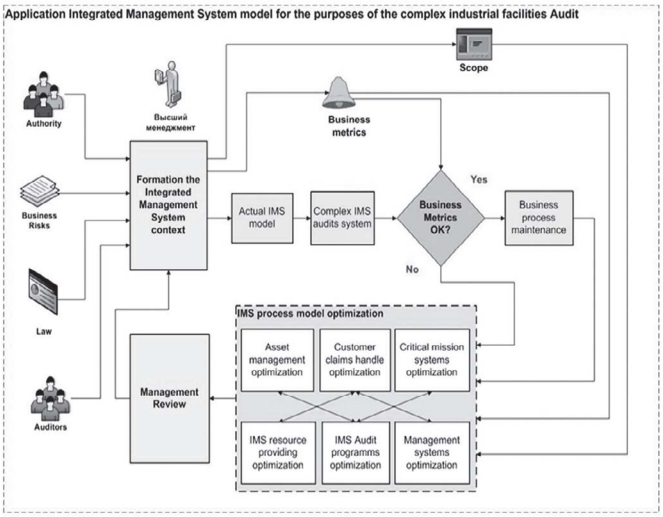

Fig.1. The IT-security management systems model for audit of airport complex

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 IT-security incidents (N*IT-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 Fig. 2.

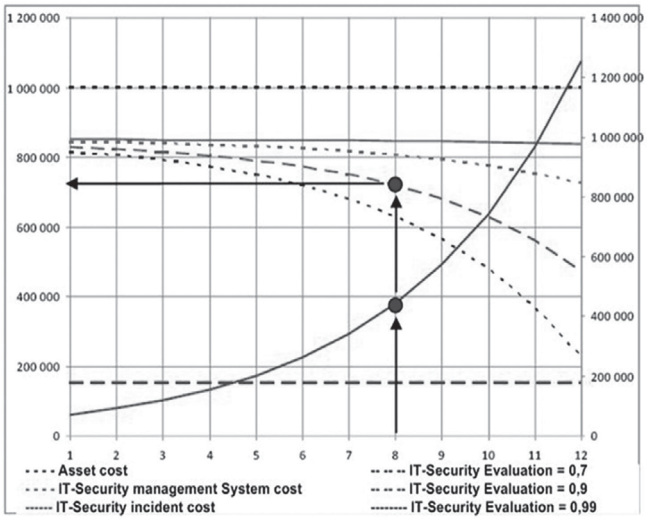

Fig..2. Assessment of economic efficiency of IT-security management systems

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:

$$A_{ISM} = C_{asset} - C_{control} - C_{incident}*(1 - P_{IMS)} = 1000000 - 180000 - 420000*0.3 = 694000$$

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:

$$A_{ISM} = C_{asset} - C_{incident} = 1000000 - 420000 = 580.000$$

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. Note that the reduction of N *IT-security* increases objectively assessment the performance of the ISMS P_{IMS}, as a factor in reducing the impact.

VII. THREATS TO INFORMATION SECURITY WITH PERSONAL DATA

Concern about internal threats of information security to date. Government agencies and senior management of the organizations put on the first leak, as the negative consequences of this incident are obvious: direct financial losses, impact on reputation, loss of customers

According to the documents submitted in the Automated system of ensuring legislative activity (ASSD), an updated Federal law shall enter into force from 1 July 2017.

Today for such violations establishes liability in the form of a warning or a fine from 300 to 500 rubles for citizens, from 500 to 1000 rubles - for officials and from 5 thousand to 10 thousand rubles - for legal entities.

The bill proposes to strengthen the administrative responsibility for breach of law No. 152-FZ ("On personal data"). The authors of the bill believe that the current article does not allow to protect the rights and interests of citizens fully, and does not account for the severity of negative effects fully. It is therefore proposed to increase the size of administrative fines several times.

According to the draft law, submitted for the third reading, processing data not in accordance with the law and for the use of this data is not misused, the offender is a private person may receive a warning or a fine in the amount from 1 thousand to 3 thousand rubles. However, an official paid from 5 thousand to 10 thousand rubles, and legal person - from 30 thousand to 50 thousand rubles.

The processing of personal data without the consent of the citizen will lead to the imposition of a fine in the amount from 3 thousand to 5 thousand rubles for citizens, from 10 thousand to 20 thousand rubles - for officials and from 15 thousand to 75 thousand rubles for legal entities.

If the data controller has not published information not provided access to the document, which defines all of the terms of use of the personal information or data on implemented requirements, he will be given a warning or issued an administrative fine. For citizens it will make from 700 to 1500 rubles, for officials - from 3 thousand to 6 thousand rubles for individual entrepreneurs (IP) - from 5 thousand to 10 thousand rubles, and for legal entities - from 15 thousand to 30 thousand rubles.

In addition, the administrative penalty is imposed for failure to comply with the data controller of the requirements of the data subject to clarify personal data, their blocking or destruction. For citizens it will lead to an administrative fine in the amount from 1 thousand to 2 thousand rubles, for officials - from 4 thousand to 10 thousand rubles., for individual entrepreneurs - from 10 thousand to 20 thousand rubles, for legal entities - from 25 thousand to 45 thousand.

According to the draft law, the data controller, do not use in the processing of such data special means of

automation, will be fined, and if you do not comply with the conditions for storage of material carriers of personal data to prevent unauthorized access to them. But only if this resulted in improper or accidental access to personal data, destruction, change, blocking, copying, provision or dissemination.

In this case, once it is subject to a fine from 700 to 2000 rubles for citizens from 4 thousand to 10 thousand rubles - for officials from 10 thousand to 20 thousand rubles for individual entrepreneurs and from 20 thousand to 50 thousand rubles for legal entities.

For failure to comply with state or municipal personal data operator requirements for data masking provides a warning or a fine for officials in the amount from 3 thousand to 6 thousand.

VIII. Application of the Theory of Elite Groups to Select IT-Security Metrics

To form the best possible solutions in terms of the task set of information security metrics are encouraged to apply certain provisions of the theory of "elite groups" (proposed by prof. A. Efimov) [22], complemented by the selection rules, rotation and drop-out elements in relation to the PDCA cycle. There is a set of a countable set of Y elements (for the purposes of this publication - the set of IT-Security metrics). The property of each element is expressed in a certain criterion value y_i, being in the range $0 \le y \le 1$, and it is known that the larger the value reaches y_i, the better. In particular, these requirements exactly corresponds to the problem of estimating the specific attribute - the better its "absolute" rating, the better and the more general assessment of the effectiveness of the ISMS measurement.

Known goal: $0 \le \alpha \le 1$ and known demand - the goal on the condition that a certain quality score was not lower than a predetermined value $\alpha \le 1$. The problem is formed as the selection of the source of Y predetermined number of elements (IT-Security metrics) to achieve this goal with specify quality indicator. The set Y may be present elements y_i, for which the $y_i \ge \alpha$ (called "elite" items) and $y_i \le \alpha$ (called "weed" elements).

The proposed method is also recommended for experts to carry out selection of elements y_i accident that is, firstly, the requirement of the standard [19] for the formation of a "sample audit» (audit sample) and, secondly, to rule out, in practice, cases of "fitting" of the set Y elements under predetermined result α. Thus, the quality of the distribution of Y in a certain "elite" group can be characterized by the distribution density [22]:

$$F_{Elite\ New}(y) = \left\{ \gamma \frac{\beta}{F(\alpha)} f(y): y < \alpha; (1-\gamma) \frac{1-\beta}{1-F(\alpha)} f(y): y \ge \alpha \right\}$$

where:

α – quality;

β – probability of selection in the "elite" group of "weed" elements;

γ – probability of selection in the “elite” group elements, which never been selected before;

F (y) – distribution function y quality in the original group;

f (y) – the corresponding density function.

It is important that if a number of reasons the elements selected "elite" group may be retiring, but want to save the "representativeness" of the audit sampling [19] for measuring purposes (e.g. for measuring purposes in the process of auditing information security a certain fixed amount of ISMS processes and / or IMS), it is necessary to solve the problem of re-select items from the remaining core set of Y. the new algorithm proposed use of "elite groups" for performance measurement purposes ISMS is shown in Fig. 3.

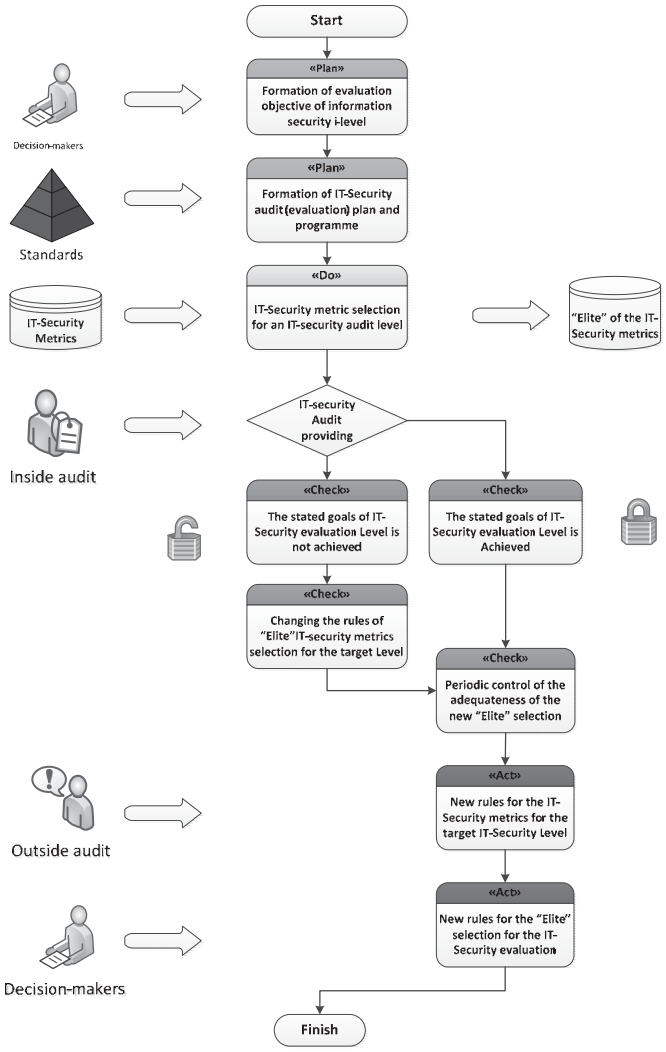

Fig. 3. Algorithm for the formation of IT-Security metrics on the basis of the theory of "elite groups"

In the new proposed algorithm introduced new functions in strict accordance with the PDCA cycle (Deming cycle). It is recommended to take into account (for the purposes of this publication with respect to the audits of the ISMS), a number of new developments:

- It is necessary to focus primarily on the proportion of "elite" elements satisfying $y_i \ge \alpha$, but not previously selected for the audit;

- It is necessary to monitor the behavior of the "quality" of each selected "elite" element, if there are sufficient resources - the totality of the "elite" of the elements, including "Reserve" of the set Y;
- It is necessary to form the rules for the selection, rotation and drop-out "elite" members (in practice, this means reviewing information security metrics on the basis of, for example, the internal ISMS audit and / or IMS).

IX. CONCLUSION

It is shown that the ultimate goal of applying set of IT-security controls is evidence 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.

The proposed method of forming the numerical IT-Security metrics is a further development of the existing methods of performing audits in accordance with the well-known ISO 19011 and ISO 27004 standards and is designed to measure the effectiveness of the ISMS with a view to ensuring a given level of security decision-makers.

REFERENCES

[1] Rudakov SA The concept of selection of information security metrics, *State University Journal of Marine and River Fleet them. Admiral SO Makarova.* 2013, Vol. 3 (22). pp. 162-166.

[2] Zefirov S., Golovanov V. Information security management system and measurement. Metrology, metric, safety, *Information Security. Inside.* 2008, № 2 (20). pp. 22-27.

[3] Kotenko I., Yusupov R. Perspective directions in the field of computer security research. *Information Security. Inside.* 2006, № 2 (8). pp. 46-57.

[4] Petrenko SA SOX 404 requirements for the IT control, *Information Security. Inside.* – 2006, № 3 (9). pp. 10-16.

[5] The Global State of Information Security Survey 2016 [electronic resource]. - Access: www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml/ free (reference date 18/04/2016)

[6] Center for strategic and International Studies [electronic resource]. - Access: www.csis.org free (reference date 18/04/2016).

[7] The official website for Infosecurity Russia [Electronic resource]. - Access: www.infosecurityrussia.ru/2015/program/23.09.2015/?lang=ru#s22083 free (reference date 18/04/2016).

[8] Security Report [Electronic resource]. https://www.trustwave.com/Resources/Library/Documents/Security-on-the-Shelf-An-Osterman-Research-Survey-Report/ free (reference date 18/04/2016).

[9] White Paper «Dealing with Data Breaches and Data Loss Prevention» [Electronic resource]. - Access: https://www.proofpoint.com/de/id/PPWEB-WP-Osterman-Data-Breaches-and-DLP-Q115 free (reference date 18/04/2016).

[10] Livshits I. The urgency of the application of information security metrics to assess project performance information security management systems, *Quality Management*. 2015, Vol. 1. pp. 74 - 81.

[11] Livshits I. Approaches to solving the problem of taking into account losses in the integrated management system, *Informatization and Communication.* 2013, Vol. 1. pp. 57 - 62.

[12] Livshits I. The approaches to the use of an integrated management system model for the audit of complex industrial facilities - airport complexes, *Proceedings SPIIRAS.* 2014, Vol. 6. pp. 72 - 94.

[13] ISO / IEC 27000: 2014. Information technology - Security techniques - Information security management systems - Overview and vocabulary, International Organization for Standardization, 2014. p.31.

[14] ISO / IEC 27001: 2013. Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization, 2013. p.23.

[15] ISO / IEC 27004: 2009. Information technology - Security techniques - Information security management - Measurement, International Organization for Standardization, 2009. p.55.

[16] ISO / IEC 27005-2011. Information technology - Security techniques - Information security risk management, International Organization for Standardization, 2011. p.68.

[17] Federal Information Security Management Act (FISMA) [electronic resource]. - Access: www.csrc.nist.gov free (reference date 18/04/2016).

[18] ISO [electronic resource]. - Access: http://www.iso.org/iso/annual_report_2014_en_-_lr.pdf free (reference date 18/04/2016).

[19] GOST R ISO 19011: 2011. Guidelines for auditing management systems. Moscow, Standartinform 2013.

[20] GOST R 52447-2005 Information Security. information protection technique. Nomenclature of quality indices, Moscow, Standartinform 2006, p.23.

[21] Number of U.S. government 'cyber incidents' jumps in 2015 Reuters [electronic resource]. - Access: http://www.reuters.com/article/us-usa-cyber-idUSKCN0WN263 free (reference date 10/08/2015).

[22] Efimov A. Elite group, their origin and evolution. *Knowledge is power.* 1988, Vol. 1. pp. 56 - 64.