ISSN 1407-7493

COMPUTER SCIENCE
DATORZINĀTNE

2008-34

APPLIED COMPUTER SYSTEMS
LIETIŠĶĀS DATORSISTĒMAS

CONCEPT OF INFORMATION SECURITY SYSTEM EVALUATION MODEL

Dmitry Kryukov, *Riga Technical University,*
Meza 1/3, Riga, LV 1048, Latvia, M.Sc.ing.,
dmirijs.krjukovs@gmail.com

Eleonora Latiseva, *Riga Technical University,*
Meza 1/3, Riga, LV 1048, Latvia, asoc. prof., Dr.sc.ing.,
elatiseva@cs.rtu.lv

Information security, evaluation, model, controls.

1. Introduction

As a result of explosion of information and communication technologies during last decade business dependence on reliable and secure functioning of Information Communication Technologies (ICT) has boomed. It would be difficult to find a business that has not been touched by information technology and dependent on information it processes. Information systems have become pervasive in global society and business, and the dependence on these systems and the information they handle is arguably absolute. Availability, integrity and confidentiality of organisation owned information becomes a key factor in ensuring competitive advantage and mission critical factor for successful and effective functioning of business processes. Business should consider that information security plays support role for organisation goal achievement and is not only a technological issue. It affects all levels of organizational hierarchy – from organisation's governance level where business strategy, budgeting and structure is defined to operational level where software-technological, physical, environmental and procedural controls related to information security are implemented and managed.

Accurate, quantitative, objective and comparable assessment of information security system's operation in organization gives possibility to analyze, baseline, compare and optimize information security function in organisations to effectively support business processes in organization's goal achievement. Assessment should provide results not only about technological solution's implementation effectiveness, but should in its turn provide measurable quantitative results of how efficiently information security is functioning in

organization, how it is aligned with business strategy to support organizational objectives, how existing situation and implemented solution's effectiveness is measured and analyzed, how risks are managed and finally how effective are implemented controls.

At the moment there is no unified information security evaluation framework which allows measuring whole information security system effectiveness in organisation from strategic, tactical and operational perspectives. All existing approaches cover only some stages of information security evaluation, e.g. implementation of technical controls, effectiveness of IT general controls or maturity level of organisation's information security processes.

To help understanding of proposed unified model for organisation's information security system evaluation the system's functioning principle is described below.

2. Information security systems' functioning model

Information security covers all information process, physical and electronic, regardless of whether they involve people and technology or relationships with trading partners, customers and third parties. It is concerned with all aspects of information and its protection at all points of its life cycle within the organization.

Information security ensuring in organisation is a cyclic process of evaluating of current state in information security and improving it by determining elements which needs improvements, finding appropriate solutions and implementing them.

Information security system's functioning process is iterative (cyclic) and realizes risk management practises which include risk identification and prioritization, development and implementation of countermeasures and controls to minimize risk and residual risk assessment activities.

Information security system is functioning on all organisations' hierarchical levels. The following levels of information security system and major responsibilities are defined:

- Governance level. This level is very relevant to business objectives and strategy. Some objectives of information security governance level are: information security alignment to business strategy, high level business risk management, strategic decision making and budgeting. Responsibility for governance level correct functioning lies on top management.
- Management level. This level's responsibilities include management of organisational-coordination measures such as management and quality assurance of implemented and planned controls (solutions) according to defined tasks and information security strategy and policy, indicators of functioning of controls development and report analysis, analysis of risks to information security and reporting to top management (governance level). Tactical decisions are made at management level.
- Operational level. At this level executive implementation and maintenance of controls and countermeasures according to decisions made at management level is performed. Scope of controls implemented to minimize risks consists of physical and environmental controls, procedural controls and software-technical controls (solutions). At operational level measurements of control's functionality according to defined indicators is being performed and reported to upper management level for analysis and decision making.

The conceptual information security system's functioning model and collaboration between levels is shown on Figure 1.

In order to describe information security evaluation's model performance information security system's levels should be described in more details.

2.1. Governance level

IT Governance institute in its Control Objectives for Information and related Technology defines governance as "a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes" [4].

At this level integration of information security governance into the overall enterprise governance framework take place. Strategic decisions are made on how information security and IT supports business processes and what relations are between them [3].

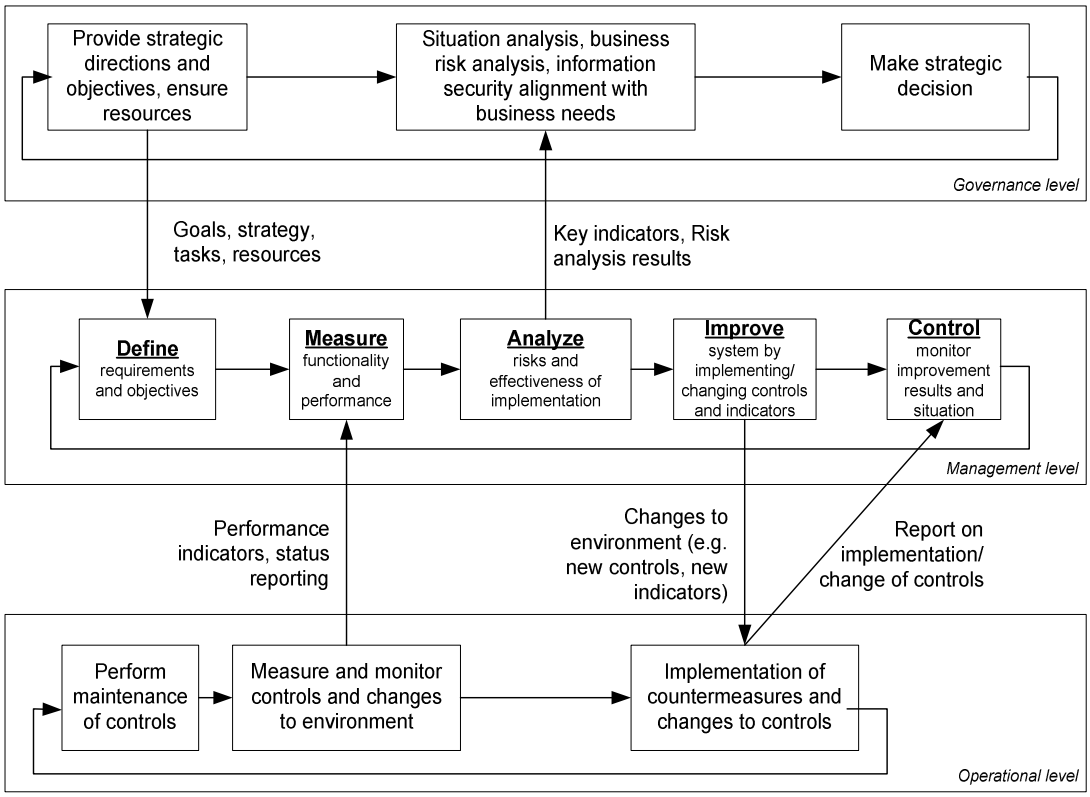

Figure 1. Conceptual information security system's functioning model

Information security strategy is defined in support of business strategy and direction. At governance level top management define what role and priority for information security is designed in context of whole organisation roles and priorities [7]. Top management commitment and support for information security as well as their vision of the desired state of information security in organisation, what is allowed, what is not, how risks should be managed and how environment should be controlled results in high level documents such as information security policy.

At governance level top management defines medium and long term goals and tasks of information security and IT for responsible departments. Key performance indicators for information security are received from management level and analyzed in context of whole organisation development strategy, achieved current state and desired state.

Results of risk analysis and key performance indicators as well as financial indicators of information security operation provide the base for making strategic decisions, set new objectives, define constraints and provide resources (both financial and people) to achieve defined objectives.

2.2. Management level

The objectives of information security management level are to perform organisational-coordination measures, control and direct operational level, accomplish defined tasks and develop tactical plans to achieve defined objectives according to information security strategy and policy.

Stages of information security management level are very similar to Six Sigma Improvement process. This process with some constrains may be used to control and improve quality of the underlying operational level according to directions provided from the upper governance level of organisation. In the same way as in Six Sigma improvement process we define information security management process consisting of 5 stages: Define, Measure, Analyze, Improve and Control.

At the "Define" stage responsible structures receives from the upper governance level goals to achieve and directions to follow. To fulfil the defined tasks and perform functions top management provides resources (budget). The outputs of this stage include:

- A clear statement of goals and how to measure them;
- Key quality characteristics (key drivers of top management satisfaction).

The goal of the "Measure" stage is to focus improvement effort by gathering information about the current situation. Indicators of implemented controls' functionality and performance (feedback) are received from operational level. Information about what, how and when should be measured is defined at this stage.

At the "Analyze" stage risk analysis and business impact analysis is performed to diagnose how efficiently implemented controls are functioning, what residual risks are and what possibilities to reduce risks to acceptable level are. At that stage possible changes to environment are defined such as countermeasures and controls. The results of such analysis and proposed solutions are reported to governance level. Tactical decisions within management level of authority are made to improve current situation.

The goal of the "Improve" stage is to develop, try out and implement solutions (controls and countermeasures) that address root causes. At this stage only activities needed to implement solutions and implementation management activities are performed, exact implementation process is performed at operational level. The outputs of this stage include:

- Actions to eliminate or reduce the impact of the identified root cause (risks);
- Analysis that shows how much of the initial gap was closed;
- A comparison of the plan to the actual implementation.

The goals of the "Control" stage are to maintain the gains made by improving environment, anticipating future improvements and monitoring results of improvement. Operational level at this stage reports to management level current situation with newly implemented changes and how they affect other controls.

2.3. Operational level

The objectives of information security operational level are implementation of changes to production environment initiated by upper management level, performing maintenance and configuration of implemented technical controls, measure and report results of monitoring according to defined performance indicators.

According to decision made at management level controls or countermeasures are implemented, monitored and measured at operational level in order to minimize risk identified through risk analysis made during "Analyze" stage at management level.

Controls are divided into following categories:

1. ICT infrastructure technical controls. These are software and hardware solutions implemented throughout different levels of ICT infrastructure. Examples of such controls are firewalls, intrusion detection systems, endpoint security solutions, vulnerability management systems, data encryption etc.
2. Procedural and manual controls. That group includes controls such as policies, procedures, regulations, security awareness programs or predefined activities aimed to reduce the potential risk. Such controls are non-technical and are defined throughout the organisation.
3. Physical and environmental controls. These controls address physical security and environmental issues. Examples include access cards systems, video surveillance, climate control, fire and smoke detectors.

Operational level's activities include implementation, management and measuring of controls' efficiency to minimize risk to information's confidentiality, integrity and availability.

These controls may directly address the risk or may be compensating controls that mitigate the effect of occurrence [5]. Implementation of controls and countermeasures should be part of the overall organisation's risk mitigation approach.

3. Model for information security assessment

The proposed model for assessment of organisation's information security level consequently and quantitatively evaluates effectiveness of three organisation's information security functional levels described above.

Assessment process is performed by checking both the effectiveness by design and the effectiveness by implementation of defined information security system's elements for each hierarchical level. The assessment groups of criteria reflect structure of information security system's functioning model and evaluate effectiveness of elements on all levels. The value of group of criteria which is accumulative indicator is calculated by computing average value of evaluations for each group of criteria.

Effectiveness by design reflects how well specific element, process or group of controls is designed and how effective it should be if it is correctly implemented, configured and functioning.

Effectiveness by implementation shows how well elements of information security system are implemented – are defined procedures been followed, are controls functioning directly as how they are designed to function and how technical controls are configured.

Detailed description for criteria and groups is provided below for each level of evaluation model. Each criterion accumulates number of logically grouped tests and checks to perform in order to evaluate it. Each test is rated according to range and principle described in section

3.1. Evaluation process. The graphical notation of proposed assessment model is depicted on Figure 2.

3.1. Evaluation process

The quantitative results are achieved by rating each criterion from group of criteria. Possible qualitative and corresponding quantitative values for evaluation are:

- 0 – Not effective. Element's design or implementation is non functional or such element doesn't exist in organisation's information security system.
- 0.33 – Partially effective; Information security system's element is designed or implemented poorly and don't satisfy requirements.

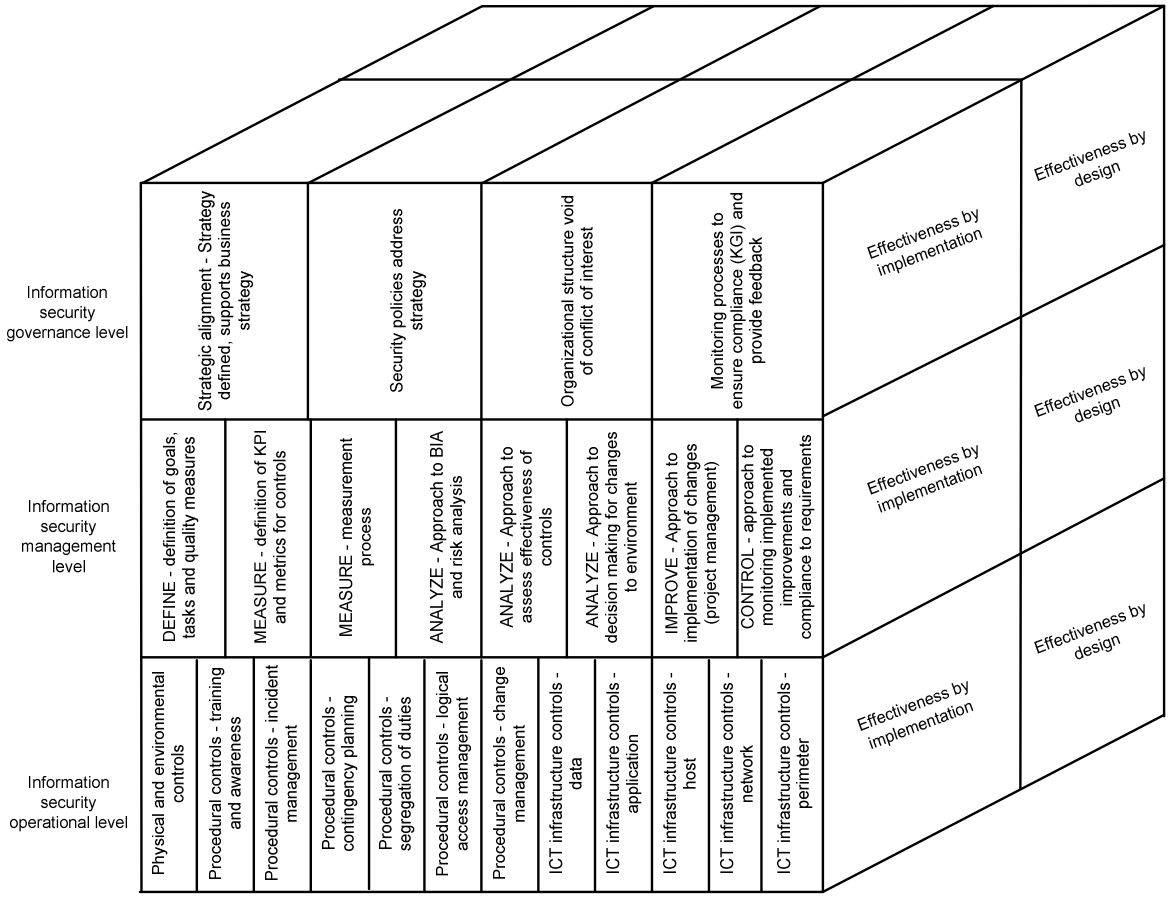

Figure 2. Conceptual information security assessment model

- 0.66 – Mostly effective. Information security system's element is well designed or implemented although few significant functional shortcomings exist.

- 1 – Fully effective. Information security system's element is well designed or implemented, no significant functional shortcomings exist.

After each criterion is rated the value for each group of criteria should be calculated using formula (1).

$$E = \frac{\sum_n i_n}{n} \times \frac{\sum_n d_n}{n}, \text{ where} \quad (1)$$

E – accumulative effectiveness of group of criteria.

n – number of elements (criterions) in group.

d_n – assessment value for n-th element (criterion) in group of criteria for effectiveness by design.

i_n – assessment value for n-th element (criterion) in group of criteria for effectiveness by implementation.

The use of following formula (2) is proposed for calculation of quantitative value of effectiveness for each level of information security in organisation:

$$\bar{E} = \frac{\sum_k E_k}{k}, \text{ where} \quad (2)$$

$\bar{E}$ – effectiveness indicator for corresponding information security assessment's level;

E_k - accumulative effectiveness of k-th group of criteria;

k – number of groups of criteria.

The $\bar{E}$ value is the resultant assessment's value for each level of information security assessment model.

In order to rate effectiveness by design d_n of elements from each group of criteria the walk-through of each element, process or control should be performed and analysis in order to identify potential cases when such element (process or control) may be ineffective or be bypassed or someone could get around it. Existence of compensating controls which increase effectiveness of element's design should be taken into consideration when performing such analysis.

Rating of effectiveness by implementation i_n for elements is based on review of existing functionality for controls, evidences of functioning for processes or resultant documents. The results of such review reflects degree to which implementation of specific element complies with its design.

3.2. Evaluation of governance level

The goal of this level of assessment model is to understand how effectively information security governance is organised and integrated into the overall enterprise governance.

To assess information security governance the following four groups of criteria are proposed to be evaluated and ranked:

1. Strategic alignment. This group of criteria allows evaluation of defined information security strategy and the process for its development, approval, implementation, and maintenance to ensure that it supports the organization's strategies and objectives.
2. Security policy. This group of criteria allows evaluation of the organization's security policies and standards and the processes for their development, approval, implementation, and maintenance to ensure that they support the strategy and comply with regulatory and legal requirements.

3. Organisational structure. This group of criteria allows evaluation of organizational structure and human resources (personnel) responsibilities for information security to ensure that they support the organization's strategies and objectives and void of conflict of interest.
4. Control of information security. This group of criteria allows evaluation of the effectiveness of information security governance control over the decisions, directions, and performance of information security so that it supports the organization's strategies and objectives.

3.3. Evaluation of management level

This level of proposed assessment model evaluates how effective are information security management processes. Evaluation criteria are based on Six Sigma improvement process and evaluate effectiveness of information security management processes described above.

Authors propose to assess management level of information security by evaluating effectiveness according to the following criteria:

1. Definition of information security goals;
2. Definition of performance indicators for controls.
3. Measurements of indicators for controls.
4. Approach to perform business impact analysis and risk analysis.
5. Assessment of effectiveness of controls.
6. Approach to improvement solution development.
7. Solution implementation management.
8. Control over implemented improvements.

3.3. Evaluation of operational level

Assessment of operational level is achieved by evaluating each group of controls by performing analysis of its design and implementation. It's proposed to organize groups of controls into categories as follows:

1. ICT infrastructure technical controls [1]
    a. Controls implemented at perimeter level
    b. Controls implemented at network level
    c. Controls implemented at host level
    d. Controls implemented at application level
    e. Controls implemented at data level
2. Procedural and manual controls
    a. Change management
    b. Logical access management
    c. Segregation of duties
    d. Contingency planning
    e. Incident management
    f. Training and awareness
3. Physical and environmental controls

3.5. Applicability of proposed model

The proposed concept of information security system evaluation model in order to be successfully implemented and to bring added value to customers requires development of detailed controls and criterions for each group of controls and criterions defined above. A testing methodology and number of tests that will follow this methodology and support detailed controls and criteria should be developed as well.

The proposed model after development of detailed test methodology could assist in performing some of the following tasks:

1. Third party reporting for organisations that have decided to outsource its own processes or just data processing. Third party reporting is aimed to stakeholders of outsourced business processes who require timely information about controls in place and their operating effectiveness. Although many organizations provide reports like SAS70 to clients these reports cover the objectives of a financial statement audit and they do not cover important control information about information security, privacy, or other non-financial objectives about which stakeholders may be concerned.
2. Assessment of information security of organisation by internal or external auditors. This allows identifying poorly designed or implemented information security system's elements and controls on all levels and provision of accurate recommendations which should be implemented in order to achieve the desired level of information security.
3. Increasing the level of information security by introducing missing technological controls, improving or introducing missing elements of information security management and governance as well as aligning information security with business objectives.
4. Baselining of information security and comparison of the state of information security systems between different organisations without making confidential information about internal controls and solutions available to other organisations.

3.6. Alternatives for information security assessment

Some other alternative approaches and models to assess information security in organisation are available. Most of them are based on conventional information security risk assessment [2] and are not focused on support for information security governance and achievement of organisation's business objectives. Nevertheless some existing methods and approaches to information security risk assessment (e.g. described in [2]) might be used as a base for development of testing methodology and tests to support the proposed model.

The following alternatives to proposed assessment model could be mentioned – CobiT Maturity model and US National Security Agency (NSA) Infosec Assessment Methodology (IAM) criticality model [6]. Unlike the NSA IAM model, which is only focused on data and systems and CobiT Maturity model [4], which is focused on maturity of processes, a richer picture of the entire organization's security program is provided in proposed model due to the approach to assess all levels involved in ensuring information security in organisation – governance, management and operational both from design and implementation points of view.

4. Conclusions

Quantitative assessment of information security system leads an organization to better understanding of its security system and allows defining its strong and weak elements and identifying zones of increased risks. Assessment is an important measure when comparing one organization to another or to some predefined baseline. It allows assessing the degree of trust that can be placed with interconnected computer systems between different organizations.

The proposed model for information security assessment allows quantitatively evaluate design and implementation of elements of information security system. Results of such assessment can be used to identify weaknesses in organisation's approach to information security and related risks to business. Results obtained can be used for existing information security system's improvement by redesigning, implementing or tuning weak elements (e.g. procedures, controls) if such elements are found ineffective by design or by implementation accordingly. The proposed assessment model can be used for evaluating of potential business partner in case exchange of sensitive information or interconnection of key IT systems is planned. Assessment of information security according to the proposed model may be performed by internal auditors (in case of self-assessment) or by external independent audit company.

The proposed model was developed using top-down approach starting with research of information security role in enterprise, its functioning model, existing assessment methodologies and information security coverage by these methodologies. After reviewing existing approaches, a proposed concept of assessment model was developed to cover all identified requirements of information security system in organisation.

This work has been partly supported by the European social Fund within the National Programme "Support for the carrying out doctoral study programme's and post-doctoral researches" project "Support for the development of doctoral studies at Riga Technical University".

References

1. Ashley M, StillSecure. *"Layered Network Security 2006: a best-practices approach"* // Internet, http://www.stillsecure.com
2. Douglas J. Landoll. "*The Security Risk Assessment Handbook*", Auerbach 2006.
3. IT Governance institute *"Board Briefing on IT Governance"* // Internet, http://www.itgi.org
4. IT Governance institute „*CobiT*" // Internet, http://www.itgi.org
5. Information Systems Audit and Control Association *„Certified Information Security Manager Review Manual 2006"*
6. National Security Agency homepage // Internet, http://www.nsa.gov
7. Information Systems Audit and Control Association homepage // Internet, http://www.isaca.org

Krjukovs D., Latiševa E. Informācijas drošības sistēmas novērtējuma modeļa koncepcija
Šīs raksts definē kvantitatīva informācijas drošības sistēmas novērtējuma svarīgumu un nozīmi organizācijas biznesa procesu atbalstam un apraksta piedāvāta novērtējuma modeļa koncepciju. Novērtējumam jāņem vērā ne tikai tehnoloģisko elementu realizācijas efektivitāti, bet jāspēj novērtēt informācijas drošības sistēmas funkcionēšanas efektivitāti, cik tā ir saskaņota ar biznesa stratēģiju atbalstot organizācijas mērķu sasniegšanu,

kā esošā situācija un realizēto risinājumu efektivitāte tiek mērīta un analizēta, kā tiek pārvaldīti riski un cik efektīvas ir ieviestas kontroles. Rakstā tiek dots informācijas drošībassistēmas funkcionēšanas modeļa apraksts, detalizēti apskatot katra hierarhijas līmeņa elementus un darbības. Ir definēti 3 hierarhijas līmeņi – pārvaldības, vadības un operacionālais. Piedāvātā modeļa koncepcija kvantitatīvi vērtē informācijas drošības funkcionēšanas modeļa elementu efektivitāti pēc projektējuma un realizācijas katram hierarhijas līmenim izmantojot piedāvātus kritērijus. Rakstā ir definēti informācijas drošības kritēriju grupu un gala vērtējumu izskaitļošanas principi, kā arī aprakstītas saņemto rezultātu pielietošanas iespējas.

Kryukov D., Latiseva E. Concept of information security system evaluation model

Paper defines importance and significance of quantitative information security system assessment to support organization business processes and describes the concept of proposed assessment model. The assessment should take into consideration not only effectiveness of technological solution's implementation, but should evaluate effectiveness of how information security system is functioning, how it is aligned with business strategy to support objectives, how existing situation and implemented solution's effectiveness is measured and analyzed, how risks are managed and how effective implemented controls are. Description of information security functioning model with detailed review model's elements and activities of each hierarchical level is provided in paper. Three hierarchical levels are defined – governance, management and operational. The proposed model quantitatively evaluates effectiveness by design and implementation of information security functioning model's elements for each hierarchical level using proposed criteria. Rules for evaluation of information security criteria and final assessment value as well as possibilities to use achieved results are described in paper.

Крюков Д., Латышева Е. Концепция модели оценки системы информационной безопасности

Данная статья определяет важность и значение количественной оценки системы информационной безопасности для поддержки бизнес процессов организации и описывает концепцию предлагаемой оценочной модели. Метод оценки должен учитывать не только эффективность реализации технологических элементов, но также должен быть способен оценить эффективность функционирования системы информационной безопасности, насколько она согласована с бизнес стратегией и поддерживает достижение целей организации, как измеряется и анализируется существующая ситуация и эффективность реализованных решений, как организовано управление рисками и насколько эффективны введенные контроли. В статье дается описание модели функционирования системы информационной безопасности, детально рассмотрены элементы и действия на каждом уровне иерархии. Определяются 3 уровня иерархии - уровень правления, управления и операционный уровень. Концепция предлагаемой модели позволяет количественно оценить эффективность планирования и реализации элементов модели функционирования системы информационной безопасности, для каждого уровня иерархии используя предложенные критерии. В статье определены принципы оценки критериев информационной безопасности и конечного значения оценки, а также описываются возможности применения полученных результатов.