Journal of Theoretical and Applied Information Technology
15th August 2018. Vol.96. No 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMPARATIVE ASSESSMENT OF EFFECTIVENESS AMONG CORPORATE INFORMATION SECURITY PROFILES

GEORGI N. TODOROV [1*], MARINA V. VINOGRADOVA [2], GENNADII G. SOROKIN [3], ALEXANDER A. SHATSKY [4]

[1] Assistant professor, Center of Social and Economic Development, Varna Scientific Institute of the Eastern European Commonwealth – VSIEEC, Bulgaria.
[2] Dr.Sci. (Economic), Professor, Director of Research Institute of Advanced Directions and Technologies, Russian State Social University, Russian Federation.
[3] Cand. Sci. (Sociological), Associate Professor, Department of Business Informatics and Mathematics, Tyumen Industrial University, Russian Federation.
[4] Ph.D. student, Russian State Social University, Russian Federation.
E-mail*: todorov.g@protonmail.com

ABSTRACT

The article is reviewing available approaches that make it possible to solve the problem of effectiveness among information security systems. Ensuring information security has become an important element in an enterprise sustainable development. At the same time, there is an arising question of a proper assessment for an information security level and its indicators. With an example of enterprises from the same sector, the research shows that effectiveness of an information security profile is mostly the same. This makes it possible to use universal tools when companies design and establish information protection. In the review of literature, there is a discussion of identification issues of information risks and threats and a proposed comprehensive evaluation technique. Elaborating the approach, there is a further definition of maturity levels in IT infrastructure of business processes. Findings make it possible to conclude that management levels in corporate information security in the same sector are the same. Minor differences are in place because of size effects and various investment costs that a company has to establish the information security system. The analysis of results shows heterogeneous effectiveness in information security profiles among companies when their implement investment projects focused on modernization.

Keywords: *Information security, Construction sector, Security profile, Risks, Uncertainty.*

1. INTRODUCTION

The modern business style encourages companies to develop in an active way and make the most of information technologies. A rapid development, in turn, inevitably leads to uncertainty in business processes and an occurrence of new risks. Among them, information security risks have a special place. [1-2] Information security is one of the most important aspects in integrated security, both at a level of individual enterprises and organizations, and regional and national levels in general. [3]

The rapid development in information technologies requires ongoing improvements in information protection systems and an analysis of their introduction cost effectiveness. [4] An evaluation of cost effectiveness for measures to be taken to ensure information security is an important problem, a solution to which should rest upon an integrated approach that takes into account specifics of a particular company or sector. [5-8]

Information security provision is getting an important element in sustainable enterprise development. At the same time, there is an arising question of a proper assessment of a level of information security and its indicators. [9] In terms of uncertainty, inherent to the security sector, a task of a properly evaluated information protection profile is of special significance and mostly associated with building of an arithmetic model ([10-12], etc.). A quantitative analysis and modelling are

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

those tools that make it possible to identify and evaluate objective risks. Together with qualitative approaches, in evaluations of information security profiles, it is also possible to take into account subjective manifestations of threats.

In practice, solving becomes in most cases much difficult due to highly differentiated specifics of enterprises' operations. This creates methodological problems when the decision must take into account the specifics of the industry or the field of activity of companies. Therefore, in this research, we will try to show that in the same sector enterprises might use universal tools when they design and build their information protection infrastructure. Effectiveness indicators of such tools will have no significant differences. This extended position is the main hypothesis.

The aim of the research is to work out and approbate the methodology of comparative evaluation of the effectiveness of information security profiles of enterprises.

2. LITERATURE REVIEW

In today's global economy, accelerated paces in the scientific and technical development is a growing tendency. At the same time, there are higher business risks and level of possible threats. A cumulative damage resulted from information incidents has a significant impact on company capitalization. [13-14] According to some estimates, it is commensurate with an annual growth of the gross domestic product. Interestingly enough, the problem of man-caused security arrangements is 70% associated with the man-made factor. [15] Therefore, the issue of assessing the level of information security is relevant.

In this case, confidential information as a factor of economic security provision, in the first place, is getting more important. This requires protection of actors in information relationships from a negative impact. At the same time, sources and guidelines almost do not exactly specify what information we are to protect. They simultaneously arrange a field of information events, subject to protection based on assessments of vulnerability and uniqueness of information knowledge that it is difficult to reproduce (in the meaning of the information resource). Therefore, it is possible to understand information security as an integral part of economic one. [16] It is because of this will be implemented this study.

Despite a significant number of research papers [17] on these issues, it would be reasonable to point out to the missing conventional approach to an assessment of effectiveness that corporate information security profiles have. This confirms the need for our research. In the literature, there are descriptions of very different factors that make evaluation difficult. Complicacy in the economic analysis of information security, as a rule, depends on the following factors [18-21]: rapid development in information technology and a variety of methods used to measure information security; inability to predict in a reliable way all the possible scenarios of an unauthorized access; insufficient reliable estimations of information resource costs, as well as monetary estimation of infringement consequences in this sectors.

Note that the methodology for an effectiveness assessment in investments in information security greatly differs from the methodology for investments in investment projects and has its inherent unique problems. [22] An assessment of alternative projects of information security provision and reasoning of the costs involved are usually based, on the one hand, on compliance with regulatory requirements, and on the other hand, a risk of disclosure. That is why there is a problem arising of a quantitative assessment of financial reasoning for investments in establishment and/or development of the information security system.

Risk differentiation by impact leads to selective segmented management of information security. Differentiation comes down to a decrease in values of high and medium risks to values typical for low risks. This makes it possible to accept such risks. [23] A managerial decision rests upon a forecast of future risk dynamics. The task of risk forecasting to ensure effectiveness in the information security system in risk life cycles is getting a priority and associated with an analysis of uncertainty. [24]

When evaluating projects on information security provision, keep in mind that these projects do not practically result with a real income. Instead, they have an indirect effect preventing a loss of funds, which otherwise would be spent on recovery of damaged or lost information resources. Hence, the projects related to information security, significantly reduce a risk level, hence, a risk premium in investment forecasting. See common approaches to risk assessments in corporate information security in Figure 1.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

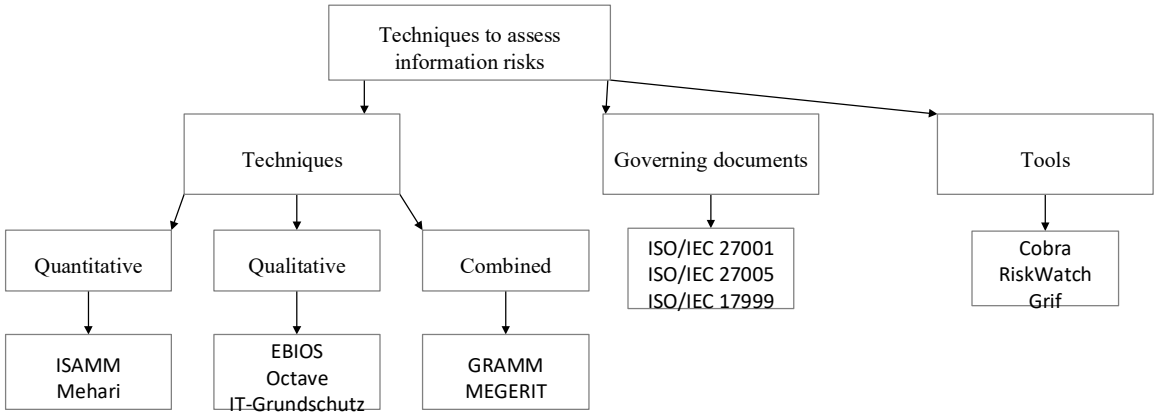

Figure 1: Approaches to risk assessment in information security

Professionals have proposed various models and techniques for a quantitative risk assessment based on fuzzy logic [25-27], linear programming [28], statistical analysis [29], Bayesian networks [30-32], neural networks [33], logic-probability modelling [34], and simulation modelling. [35-36] Equally diverse are approaches to an assessment of effectiveness for an information security profile in an enterprise.

Repin, Sakulina, and Pshekhotskaya propose to use the technique of Total Cost of Ownership (TCO) [37-39] as a basis in calculations. Miaoui and Boudriga suggest a use of the utility theory in calculations of optimal investments in security provision with considered typologies and dynamic aspects of vulnerabilities. [40] This vision has difficulties in practical implementation, because "usefulness" of the information security system does not have clear criteria and basis on subjective representation. There are several indicators that are often used to describe the utility (and in this case, to include the number of successful attacks or others), but they do not have a gradation for a strict understanding of the effectiveness of the information security profile.

Another solution goes form a parameter of information entropy. Subject to priority dynamics, an information flow must have a binding to a system formation causing a need in entropy adjustment. A capability of entropy control exactly acts as an indicator of effectiveness. [41-43] We believe that entropy can be used productively for evaluation, but this will require the collection of additional data on the parameters of the safety profile.

Obukhova and Goncharova share an alternative point of view with an approach based on a development of a composite indicator saying of an information system quality. Its meaning is a measurement of whether compared states are close. It uses the mathematical concept of distance in the environment of indicators. [44] This approach contains a mistake of subjective perception, because the distance between the id value of the indicator and the actual position is set initially by the observer.

Kashchenko [45] provides reasoned arguments in favour of criterion that shows a correlation between a decrease degree in a total information security risk and a cost of a corresponding event. If an organization decides whether a particular project is feasible, a calculation of the net present value, profit and costs that the project will bring is also the simplest case. [46] Then, effectiveness assessment model for information security investments rests upon a comparison of the net present value of costs for the elimination of consequences from threats that have come true, both in terms of introduced information protection tools and without them. The quantitative measure of efficiency through the net present value indicator is considered in our approach, but as an integral part of the integrated assessment.

Some researchers [47] tend to conclude that expert systems are the most cost-effective option for reasoning and economical evaluation of information security investments. This is because, first, it makes it possible to solve problems (that are difficult to be formalized) using the specially developed mathematical apparatus. Secondly, it makes it possible to increase effectiveness and operational efficiency of decisions taken owing to lessons learnt by experts in the field under consideration.

Ambiguous solving to the problem of effectiveness assessment for the information security profile led to a need in a development of a comprehensive formal procedure based on both quantitative and qualitative criteria that provide an adequate level of enterprise security.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. MATERIALS AND METHODS

To provide protection for an enterprise information environment, we need a systematically implemented cycle of the following steps [48-49]: analysis of risks and threats to information security; planning and development of measures to ensure information security; operational implementation of scheduled actions.

Analysing information risks, we consider all possible ways along which threats go from their source. Threat levels (P_i) required for calculations are found based on probable activation of a threat and levels of information vulnerability specific for infrastructure components along threat distribution paths:

$$P_i = P_a \times Tw_{z.z+1} \quad (1)$$

where P_a is a probability of threat materialization, $Tw_{z.z+1}$ is a vulnerability level that an information infrastructure component has.

The quantitative model of risks speaks in terms of such concepts, as event/incident frequency (ARO), expected single damage per event/incident within a period (SLE), cumulative annual damage expected from information risks and threats (ALE). The calculation is as follows:

$$ALE = ARO \times SLE \quad (2)$$

It is possible to find an expected single damage by multiplying a cost of information (AV) by the impact factor (EF). In the presented model, the impact factor refers to a size of a damage or a specific impact on a negative change in an asset value (0-1), that is, the part that the asset will lose because of an event or incident:

$$SLE = AV \times EF \quad (3)$$

Upon an initial assessment of risks and threats to information security, rank the obtained values by importance to identify low, medium, and high levels of risk. A solution to this problem is possible using quantitative scaling as an approach to an indicator with non-uniform filling in groups [50-51] or scaling with rigid boundaries. [52]

Based on components within an information and communication environment, the evaluation system should include the following: integrated index *Ia* for the development management level of the information and communication environment, including the evaluation of workflow management (*w1*), management of development processes in information systems (*w2*), management of communications (*w3*), management of staff information development (*w4*); integrated index *Ib* for the management level in prevention and counteraction of information security threats including an assessment of planning and organization of information security activities (*w5*), document security monitoring (*w6*), arrangements to differentiate an access to information assets (*w7*), organizational tools of control over operations of operating personnel and users in the corporate information system (*w8*), trainings for employees in information security basics (*w9*), adherence to safety regulations (*w10*), establishment of protection and security modes (*w11*).

In general, we will measure a level of information security (*Iib*) by the formula:

$$Iib = a \times Ia + b + Ib \quad (4)$$

Where Ia, Ib refer to integral indicators of the informatization management level and information security provision. *a, b* are priority vectors of integrated indicators of the informatization management level and information security provision.

It is necessary to evaluate an integrated indicator of informatization operations management level according to the formula:

$$Ia = \sum_{i=1}^{n} \lambda_i \times w_i \ , \quad (5)$$

where w_i are indicators that describe operations management level. λ_i are coefficients of indicator significance in the operations management level.

We will calculate an integral indicator of an operations management level to prevent and counteract materializing of information security threats as follows:

$$Ib = \sum_{i=1}^{n} \lambda_j \times w_j , \quad (6)$$

where λ_j are indicators that describe a level of operations management focused on information security threat occurrence counteraction and prevention; w_j are coefficients of indicator significance for operations management level to prevent and counteract materializing of information security threats.

Note that in order to obtain the information necessary for calculations of the indicators mentioned, the availability of the system is a prerequisite, i.e. the system that makes it possible to do monitoring over activities of an enterprise's information service.

In order to interpret the estimate, we use the Harrington scale including five intervals (Table 1).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The average numerical score by the Harrington scale is {0.90; 0.71; 0.5; 0.28; 0.10}

Table 1: Values ranked by Harrington scale

Qualitative characteristics	Value
Very high intensity of criterion property	(1.00-0.80)
High intensity of criterion property	(0.79-0.64)
Average intensity of criterion property	(0.63-0.38)
Low intensity of criterion property	(0.37-0.20)
Very low intensity of criterion property	(0.19-0.00)

We propose to interpret obtained results using the following scale. There is a critical level with a high probability of crucial losses of assets or a complete loss of a company's image in the market, which makes its further activity impossible. There is a low level with a high probability of large losses of assets and a significant damage to the company's image in the market. Next, there is an average level with an average probability of significant asset losses or a significant damage to a company's image. There is then a high level with possible moderate losses of assets or an insignificant influence on a company's image. The last one is a very high level with a low probability of lost assets or a low influence on a company's image.

4. RESULTS

In this research paper, we are going to state that enterprises from one sector might use universal tools when they design and establish information protection. Effectiveness indicators of the tools will not significantly differ. To do this, we completed calculations (as an example) for enterprises from Russian construction sector. Under the research, there were the following research objects: Trest Zhilstroy-2, LLC from Omsk (Company # 1), Spetsstroymontazh, LLC from Krasnodar (Company # 2), Zhilstroy, LLC from Moscow (Company # 3), IBK, LLC from Saint Petersburg (Company # 4), and International Group, LLC from Samara (Company # 5). Selected enterprises operate in extremely challenging conditions, which negatively affect their performance and prevent further development. We compared information protection profiles of these companies using an analysis of external risks.

At the first assessment stage for the management level of information security, it is necessary to find priority vectors for components (*a, b*) by ranking (Table 2).

Table 2: Priority vectors of information security components

Index	External risk evaluation																				Specific gravity
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
a	1	2	1	2	1	1	1	1	1	1	1	1	2	2	1	2	1	1	1	1	0.42
b	2	1	2	1	2	2	2	2	2	2	2	2	1	1	2	1	2	2	2	2	0.58

Next, let us rank indicators, provided that number of factors $n=11$, number of external threats $m=20$. We measure parameter significance by giving them a rank number. The factor with the least score has the first rank. If several factors are recognised equal, they get the same rank number. Based on survey data, researchers make a composite matrix of ranks presented in Table 3.

Table 3: Ranked information security indexes

Risk / Index	*'1*	*'2*	*'3*	*'4*	*'5*	*'6*	*'7*	*'8*	*'9*	*'10*	*'11*	*'12*	*'13*	*'14*	*'15*	*'16*	*'17*	*'18*	*'19*	*'20*
w 1	1	1	2	1	1	2	1	1	2	1	3	2	1	1	1	2	2	1	2	1
w 2	4	4	3	4	4	4	4	4	4	4	2	4	4	4	4	4	4	4	4	4
w 3	2	3	4	3	2	3	2	2	3	2	2	3	2	3	2	3	1	3	1	2
w 4	3	2	1	2	3	3	3	3	3	3	1	3	3	2	3	3	3	2	2	3
w 5	7	6	5	6	7	6	5	7	7	5	7	7	5	7	7	5	7	7	5	7
w 6	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
w 7	4	3	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
w 8	3	4	3	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
w 9	6	7	6	7	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
w 10	5	5	7	5	5	5	7	5	5	7	5	5	7	5	5	7	5	5	7	5
w 11	2	1	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Then calculate risk share harmonization using the concordance coefficient:

$$W = \frac{S}{\frac{1}{12}m^2\left(n^3 - n\right) - m\sum T_i}, \quad (7)$$

$$T_i = \frac{1}{12}\sum\left(t_l^3 - t_l\right) \quad (8)$$

where m is a number of external information risks; n is a number of indexes; T_i is a number of bonds (kinds of repeated elements) in evaluations of the *i-th* risk; t_l is a number of elements in the *l-th* bond for the *i-th* risk (number of repeated elements).

Having measured concordance between information risks, as for ranks of indicators, we obtain concordance coefficient W = 0.91. This means high risk concordance. As a result, there are indicator significance coefficients as follows:

$$\lambda_{i,j} = \left\{\begin{matrix} 0,14; 0,38; 0,24; 0,24; 0,22; \\ 0,04; 0,14; 0,11; 0,22; 0,2; 0,07 \end{matrix}\right\}.$$

Let us assess the IS management level.

The calculated concordance coefficient for companies is 0.71-0.77. This means high risk concordance. Having calculated indicators with significance factors considered (Annexes 1-5), we obtained the following estimates, shown in Fig. 1.

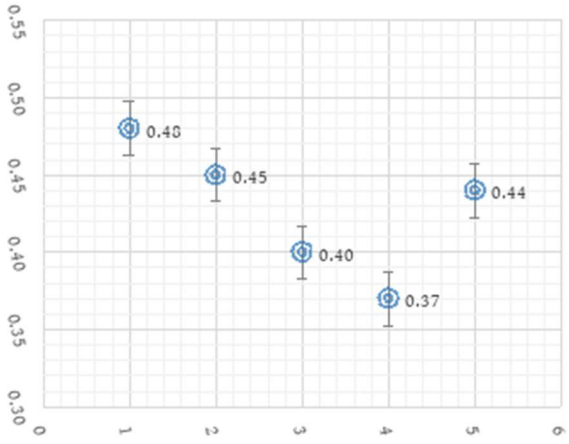

Figure 1: Assessed levels of information security management in construction companies

As it follows from the figure, average levels of information security are equal and it is typical for all the enterprises under consideration. There are high information risks observed in measures of control over workflow processes (w1) and arrangements of the protection mode (w11).

Consider a modernization project for a protection system of enterprises for a period of T years and analyse changed effectiveness of investments in the information security system.

Assign capital costs for a purchase of equipment and its installation to initial period $t = 0$ and denote by C_0. We will denote maintenance costs for year t by C_t and assign to an end of a corresponding year. Then we will found a total flow of investment costs using vector $C = (C_0, C_1, ..., C_T)$. Assign casual losses due to information incidents to the end of this year. Denote the flow of these losses in terms of the valid protection system *by* $W = (0, W_1, ..., W_T)$, while without the protection system by $L = (0, L_1, ..., L_T)$. Denote the flow of total costs, including investment costs and occasional losses from possible information incidents by vector $E = (E_0, E_1, ..., E_T)$:

$$E = C + W \quad (9)$$

To estimate the cash flow, let us apply net present value, which will be a random variable with r as a time-constant interest rate:

$$NPV\left(E\right) = \sum_{t=0}^{T}\frac{E_t}{\left(1+r\right)^t} \quad (10)$$

We assume annual casual losses as independent. Let us obtain the following formula for mathematical expectation and variance of the value:

$$M\left(NPV\left(E\right)\right) = \sum_{t=0}^{T}\frac{M\left(E_t\right)}{\left(1+t\right)^t}, \quad (11)$$

$$D\left(NPV\left(E\right)\right) = \sum_{t=0}^{T}\frac{D\left(E_t\right)}{\left(1+t\right)^{2t}} \quad (12)$$

The cited values make it possible to estimate an average net present value of total costs for protection systems and possible deviations from them. We will refer the amount of $E_{k\sigma} = VaR_{k\sigma}$, on which the maximum value of TCH costs depend with reliability $P_{k\sigma} = 1 - 1/k^2$, as $k\sigma$, cost of risk:

$$E_{k\sigma} = VaR_{k\sigma} = M\left(NPV\left(E\right)\right) + k\sigma\left(NPV\left(E\right)\right) \quad (13)$$

Table 4 includes calculations of six indexes for mentioned companies: net present value of losses in absence of protection NPV (L); net present value of total investment costs NPV (C); mathematical expectation of net present value of casual losses from information incidents M (NPV (W)); standard deviation of net present value of casual losses from information incidents σ (NPV (W)); effectiveness index three sigma $E_{3\sigma} = VaR_{3\sigma}$, (NPV); index of conditionally saved funds $S_{3\sigma} = NPV(L) - E_{3\sigma}$.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Economic indexes of companies' protection profiles

Company	NPV		M	σ	$E_{3\sigma}$	$S_{3\sigma}$
	L	C				
# 1	30478.0	95	85	49	326	30152
# 2	30478.0	44	184	79	466	30012
# 3	30478.0	347	163	60	692	29786
# 4	30478.0	333	299	173	1151	29326
# 5	30478.0	55	548	233	1301	29177

The analysis of results shows heterogeneous effectiveness of information security profiles that companies have when they run investment modernization projects. The most "expensive" security profile ensures a significant amount of conditionally saved funds. At the same time, significant investments in security profile making lead to a relatively higher overall risk index.

Research results make it possible to conclude that levels of information security management in enterprises in the same sector are identical. Minor discrepancies result from size effects and various investment costs required for an establishment of the information security system.

Comparison of the results obtained by the author's method of assessing the effectiveness of information security profiles allows us to conclude that the method has no shortcomings in approaches to reviewing the literature. Complex qualitative and quantitative evaluation removes the subjective error and allows an adequate audit of the systems.

5. DISCUSSION

The system that supports information security management in construction enterprises is a set of subsystems to control constituents of the business environment. Information security management assumes regular managerial decision making that involves a choice of certain alternatives and organizational and technical parameters of individual systems and their constituents.

The risk management methodology implies a number of options for actions, in accordance with which employees might (A) accept an information security risk. This means that a user agrees to a risk and losses associated with it. In this case, everybody continues working as usual. They also might (B) make it lower in order to make a scheduled risk magnitude lower when taking certain measures. They might (C) transfer it to compensate for a potential damage by insurance or a risk transformation into another risk with a lower value of probable occurrence and possible damage.

ISO/IEC 15504 [53] includes a model of maturity assessment, based on identified attributes of evaluated processes. Attributes are measurable characteristics for a process potential and methods of its evaluation. Maturity models rest upon the idea that a number of acquired competencies (knowledge, skills, and abilities) get their new quality. Thus, it is possible to distinguish the following maturity levels for the information infrastructure of business processes. [54-55]

First, basic level. The information infrastructure of the basic maturity level has the following typical features: low degree of processing automation, minimal centralization of management, neglected standards and security policies. At this level, there are no analysis and assessment of information security risks. Employees do not assess the information security risks for projects, solutions and strategies that they develop. Managers are not aware of possible consequences for company's activities related to making good on the threats of information security.

Second, standardization level. At this level, employees apply administration standards and policies. They use customized security policies. They have also identified information assets with a completed list of vulnerabilities and a likelihood of threats benefiting from such vulnerabilities. Employees have measured a possible damage from threats if they become real and assessed their relevance levels. They have fixed a process of risk assessment in documents and its meaning becomes known to interested staff at trainings when they learn basic safety principles [56], evaluation and analysis of information security risks.

Third, improved level. This level of maturity has such typical features, as minimal management costs, larger weight of processes and policies to support and expand business activities. Officers reduce protection to preventive measures, i.e. a response to any security threat is predictable and fast. The risk assessment methodology is very likely to ensure that employees would identify main risks, as they have already made results of activities in a process of risk assessment and analysis compliant with relevant policies, standards and/or procedures.

Fourth, dynamic level. It makes it possible to get a full understanding of a value of an information infrastructure strategy. Such understanding contributes to efficient business operations. Managers have brought risk assessment activities in an organization to a level of best practices. The chosen risk assessment strategy goes through regular improvement events with a focus on recent achievements, valid international standards

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and results of comparisons with corresponding levels that other companies have.

6. CONCLUSION

The study of basic approaches to an information security assessment made it possible to define directions for a methodological improvement of a quantitative and qualitative risk analysis in the system of information security management in construction enterprises. Main advantages of the proposed approach are assessment detailing and specification. It will make it possible with more reasons to choose measures to ensure information security in enterprises and define a maturity level of the information infrastructure in terms of external environment challenges.

Findings make it possible to conclude that levels of information security management in enterprises are identical in the same industry. Minor discrepancies depend on size effects and various investment costs for establishment of the information security system. The analysis of findings shows heterogeneous effectiveness of information security profiles in companies implementing investment modernization projects. First, the most "expensive" security profile provides a significant amount of conditionally saved funds. Second, significant investment costs in safety profile making result in a relatively higher overall risk index.

REFERENCES

[1] I.Yu. Shakhalov, A.V. Dorofeev, "The Basics of Information Security Management of a Modern Organization, Legal Informatics", No. 3, 2013, pp. 4-14.

[2] J. Wittkop, "Building a Comprehensive IT Security Program: Practical Guidelines and Best Practices", Apress, 2016, 195 p.

[3] V.N. Solyanoy, "Features in Building an Expert System for Economic Efficiency Assessment of Information Security Measures," Information and Technology Bulletin, Vol. 13, No. 3, 2017, pp. 127-136.

[4] A.I. Hohan, M. Olaru, I.C. Pirnea, "Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles", Emerging Markets Queries in Finance and Business, Vol. 32, 2015, pp. 352-359.

[5] S. Karpenko, "Information Security Economics", http://www.pcweek.ua/themes/detail.php?ID=127249,

[6] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, R. Wieringa, "An Integrated Conceptual Model for Information System", Software & Systems Modelling, February, 2018, pp. 1-28.

[7] T. Kosub, "Components and Challenges of Integrated Cyber Risk Management", Zeitschrift für die Gesamte Versicherungswissenschaft, Vol. 104, Iss. 5, 2015, pp. 615-634.

[8] L. Kralik, R. Senkerik, R. Jasek, "Model for Comprehensive Approach to Security Management", International Journal of System Assurance Engineering and Management, Vol. 7, Iss. 2, 2016, pp. 129-137.

[9] H.K. Kong, T.S. Kim, J. Kim, "An Analysis on the Effects of Security Investments: a BSC Perspective", Journal of Intelligent Manufacturing, Vol. 23, Iss. 4, 2012, pp. 941-95.

[10] B. Blakely, "Returns on Security Investment: An Imprecise but Necessary Calculation", Secure Business Quarterly, No. 1(2), 2001, p. 27.

[11] M. Al-Humaigani, D.B. Dunn, "A Model of Return on Investment for Information Systems Security", Circuits and Systems, No. 1, 2003, pp. 483-485.

[12] V.C.S. Lee, "A Fuzzy Multi-criteria Decision Model for Information System Security Investment", Lecture Notes in Computer Science 2690, 2003, pp. 436-441.

[13] S.H. Nam, "An Empirical Study on the Impact of Security Events on the Stock Price in the Analysis", South Korea, Korea University, 2006.

[14] A. Yayla, Q. Hu, "The Impact of Information Security Events on the Stock Value of Firms: the Effect of Contingency Factors", Journal of Information Technology, Vol. 26, Iss. 1, 2011, pp. 60-77.

[15] V.D. Tolmachev,"On the Staffing of the Modern Energy", Energy Safety and Energy Economy, No. 1, 2011, pp. 37-38.

[16] I.S. Shin, "Review the Economics Means to Information Security", Information Security Review, 1 (1), 2004, pp. 27-40.

[17] W.A. Cram, J.G. Proudfoot, D'Arcy, "Organizational Information Security Policies: a Review and Research Framework", European Journal of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Information Systems, Vol. 26, Iss. 6, 2017, pp. 605-641.

[18] N.O. Shevkunov, A.V. Zhigunova, "Methodical Bases of an Estimation of Efficiency of Maintenance of Information Safety", Science and Education; Facilities and Economy; Entrepreneurship; Law and Management, No. 2 (93), 2018, pp. 33-36.

[19] I.M. Azhmukhamedov, T.B. Khanzhina, "Assessment of Economic Efficiency of Measures to Ensure the Information Security", Vestnik of Astrakhan State Technical University, Series "Economics", No. 1, 2011, pp. 185-190.

[20] A.C. Johnston, M. Warkentin, M. McBride, L. Carter, "Dispositional and Situational Factors: Influences on Information Security Policy Violations", European Journal of Information Systems, Volume 25, Issue 3, May 2016, pp. 231-251.

[21] R. Baskerville, "Risk Analysis: an Interpretive Feasibility Tool in Justifying Information Systems Security", European Journal of Information Systems, Vol. 1, Iss. 2, March 1991, pp. 121-13.

[22] S. Prosnekov, "Problem of the Evaluation of Information Security Threat Realization Probability in View of Evaluation of Investment Effectiveness Process", Nauka-Rastudent, No. 5, 2016, p. 27.

[23] S.A. Petrenko, S.V. Simonov, "Information Risk Management", Moscow, DMK Press, 2004, 384 p.

[24] A.I. Kostogryzov, V.M. Lazarev, A.E. Lyubimov, "Prediction of Risks for Ensuring the Efficiency of Information Security Systems During Their Life Cycle", Legal Informatics, No. 4, 2013, pp. 4-16.

[25] H. Beheshti, M. Alborzi, "Using Fuzzy Logic to Increase the Accuracy of E-commerce Risk Assessment Based on an Expert System", Engineering Technology & Applied Science Research, Vol. 7, Iss. 6, pp. 2205-2209.

[26] Y.N. Imamverdiev, S.A. Derakshande, "Fuzzy OWA Model for Information Security Risk Management", Automatic Control and Computer Sciences, Vol. 45, Iss. 1, February 2011, pp. 20-28.

[27] S. A. Glushenko, "An Adaptive Neuro-fuzzy Inference System for Assessment of Risks to an Organization's Information Security", Business Informatics, Vol. 39, Iss. 1, pp. 68-77.

[28] I.A. Zikratov, S.V. Odegov, A.V. Smirnykh, "Information Security Risks Optimization in Cloudy Services Based on Linear Programming", Scientific and Technical Journal of Information Technologies, Mechanics and Optics, No. 1 (83), 2013, pp. 141-144.

[29] U. Saluja, D.N. B. Idris, "Statistics Based Information Security Risk Management Methodology", International Journal of Computer Science and Network Security, Vol. 15, Iss. 10, 2015, pp. 117-123

[30] N. Poolsappasit, R. Dewri, I. Ray, "Dynamic Security Risk Management Using Bayesian Attack Graphs", IEEE Trans. Dependable and Secure Computing, Vol. 9, No. 1, 2012, pp. 61-74.

[31] K. Wu, S. Ye, "An Information Security Threat Assessment Model Based on Bayesian Network and OWA Operator", Applied Mathematics & Information Sciences, Vol. 8, Iss. 2, 2014, pp. 833-838.

[32] X.-Z. Wang, "Network Information Security Situation Assessment Based on Bayesian Network", International Journal of Security and Its Applications, Vol. 10, Iss. 5, 2016, pp. 129-137.

[33] D.-M. Zhao, J.-X. Liu, Z.-H. Zhang, "Method of Risk Evaluation of Information Security Based on Neural Networks", International Conference on Machine Learning and Cybernetics, Vols. 1-6, Baoding, China, JUL 12-15, 2009, p. 1127.

[34] D.A. Kotenko, "The Method of Information Security Risk Assessment Based on Scenario-based Logic-probabilistic Modelling", Cand. Sci (Eng.), Saint Petersburg State University of Information Technologies, Mechanics and Optics, Saint Petersburg, 2010.

[35] Y.G. Kim, D. Jeong, S.H. Park, J. Lim, D.K. Baik, "Modelling and Simulation for Security Risk Propagation in Critical Information Systems", In: Y. Wang, Y. Cheung, H. Liu (Eds.), "Computational Intelligence and Security. CIS 2006. Lecture Notes in Computer Science", Vol. 4456, Springer, Berlin, Heidelberg, 2007, pp. 858-868.

[36] E. Kiesling, A. Ekelhar, B. Grill, C. Strauss, C. Stummer, "Selecting Security Control Portfolios: a Multi-objective Simulation-optimization Approach", EURO Journal on Decision Processes, Vol. 4, Iss. 1–2, June 2016, pp. 85–117.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[37] M.M. Repin, N. Poolsappasit, R. Dewri, I. Ray. "Dynamic Security Risk Management Using Bayesian Attack Graphs", IEEE Trans. Dependable and Secure Computing, Vol. 9, No. 1, 2012, p. 61-74.

[38] A.S. Katasev, D.V. Kataev, A.P. Kirpichnikov, "Neural Network Forecasting of Information Security Incidents of an Enterprise", Bulletin of Kazan National Research Technological University, Vol. 18, No. 9, 2015, pp. 215-218.

[39] A.V. Sakulina, E.A. Pshekhotskaya, "Construction of a Model for Cost-effectiveness Assessment of Information Security System", Scientific and Methodical Provision to Assessment the Education Quality, No. 2 (3), 2017, pp. 80-84.

[40] Y. Miaoui, N. Boudriga, "Enterprise Security Investment Through Time When Facing Different Types of Vulnerabilities", Information Systems Frontiers, 2017, pp. 1-40.

[41] V.N. Osin, Yu.Yu. Gromov, Yu.V. Minin, V.A. Gridnev, "Effective Distribution of Information Flows in Network Information System", Scientific Bulletin of Voronezh State University of Architecture and Construction, Series "Construction Management", No. 2 (7), 2015, pp. 142-150.

[42] O.V. Sviridenko, G.M. Androsova, "Management of Manufacture Information Flows in Light Industry Enterprises Based on Simulation Technologies", Engineering Sciences - from Theory to Practice, No. 47, 2015, pp. 34-39.

[43] E.A. Voronin, V.V. Shipilov, "Information Assessment of Tool Effectiveness for State Diagnostics and Safety Insurance in Complex Engineering Systems", Questions of Safety Theory and Systems Stability, No. 19, 2017, pp. 65-74.

[44] A.A. Obukhova, I.V. Goncharova, "Assessment of Risks and Effectiveness of Protection in Information Security Management Taking into Account Indicator Interdependence", Information and Security, Vol. 12, No. 4, 2009, pp. 577-584.

[45] A.G. Kashchenko, Yu.K. Yazov, "Vector Estimation of Information Protection Effectiveness against Leakage through Technical Channels", Information and Security, Iss. 3, 2002, pp. 107-110.

[46] V.P. Veradchuk, V.A. Beletsky. "Effectiveness Evaluation of Investing in Enterprise Information Security Based on Fuzzy Sets", Izhevsk State Technical University Bulletin, No. 1, 2011, pp. 51-53.

[47] V.N. Solyanoy, "Specifics in Making an Expert System for Economic Efficiency Assessment of Information Security Measures", ISTU Bulletin, Vol. 13, No. 3, 2017, pp. 127-136.

[48] V.V. Domarev, "Security of Information Technologies. Systems approach", Kiev, Diasoft, 2004, 992 p.

[49] A.V. Balanovskaya, R.A. Seitkereev, "A Variety of Approaches to Building an Effective Information Security System for Industrial Enterprises", Bulletin of Samara Municipal Institute of Management, No. 1, 2015, pp. 21-31.

[50] E.A. Kuzmin, "Individual Scaling and Overall Evaluation of the System Uncertainty", Modern Applied Science, Vol. 9, No. 3, 2015, pp. 34-45.

[51] E.A. Kuzmin, "Logic of Interval Uncertainty", Modern Applied Science, Vol. 8, No. 5, 2014, pp. 158-162.

[52] B.S. Yelepov, V.M. Chistyakov, "Managing Processes of Information Resource Use, Moscow, Nauka, 1989, 235 p.

[53] H. van Loon, "Process Assessment and Improvement: A Practical Guide", Springer-Verlag US, 2007.

[54] J. Kouns, D. Minoli, "Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams", John Wiley & Sons, 2011, 440 p.

[55] J.V. Carvalho, Á. Rocha, A. Abreu, "Information Systems and Technologies Maturity Models for Healthcare: A Systematic Literature Review", In: Á. Rocha, A. Correia, H. Adeli, L. Reis, M. Mendonça Teixeira (Eds), "New Advances in Information Systems and Technologies. Advances in Intelligent Systems and Computing", Vol. 445, 2016, Springer, Cham.

[56] K. G. Crowther, Y. Y. Haimes, M. E. Johnson, "Principles for Better Information Security through More Accurate, Transparent Risk Scoring", Journal of Homeland Security and Emergency Management, Vol. 7, Iss. 1, 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ANNEX

Table 1: Assessed levels of information security for Company # 1

I	Index	$w_{i,j}$	$\lambda_{i,j}$	$\lambda_{i,j} \times w_{i,j}$
Ia	*w* 1	0,8200	0.14	0.11
	w 2	0.3680	0.38	0.14
	w 3	0.6600	0.24	0,15
	w 4	0.3060	0.24	0.07
Ib	*w* 5	0.4325	0.22	0.10
	w 6	0.4325	0.04	0.02
	w 7	0.4735	0.14	0.07
	w 8	0,6365	0.11	0.07
	w 9	0,2550	0.22	0.06
	w 10	0,6260	0.20	0.13
	w 11	0.8620	0.07	0.06
Ia = 0.47, Ib = 0.49, Iib = 0.48				

Table 2: Assessed levels of information security for Company # 2

I	Index	$w_{i,j}$	$\lambda_{i,j}$	$\lambda_{i,j} \times w_{i,j}$
la	*w* 1	0.8090	0.14	0.11
	w 2	0.3240	0.38	0.12
	w 3	0.6050	0.24	0.14
	w 4	0.2950	0.24	0.07
Ib	*w* 5	0,4010	0.22	0.09
	w 6	0.4860	0.04	0.02
	w 7	0.4020	0.14	0.06
	w 8	0,6260	0.11	0.07
	w 9	0.2280	0.22	0.05
	w 10	0,6260	0.20	0.13
	w 11	0,7175	0.07	0.05
Ia = 0.44, Ib = 0.46, Iib = 0.45				

Table 3: Assessed levels of information security for Company # 3

I	Index	$w_{i,j}$	$\lambda_{i,j}$	$\lambda_{i,j} \times w_{i,j}$
la	*w* 1	0,7575	0.14	0.11
	w 2	0.3350	0.38	0.12
	w 3	0.4800	0.24	0.11
	w 4	0.2190	0.24	0.05
Ib	*w* 5	0.3900	0.22	0.08
	w 6	0.4120	0.04	0.02
	w 7	0.2850	0.14	0.04
	w 8	0.6050	0.11	0.07
	w 9	0.2100	0.22	0.05
	w 10	0.5945	0.20	0.12
	w 11	0.6380	0.07	0.04
Ia = 0.39, Ib = 0.42, Iib = 0.40				

Table 4: Assessed levels of information security for Company #4

I	Index	$w_{i,j}$	$\lambda_{i,j}$	$\lambda_{i,j} \times w_{i,j}$
la	*w* 1	0,7280	0.14	0.10
	w 2	0.3460	0.38	0.13
	w 3	0.4550	0.24	0.10
	w 4	0,1900	0.24	0.05
Ib	*w* 5	0,2480	0.22	0.06
	w 6	0.3900	0.04	0.02
	w 7	0,2500	0.14	0.03
	w 8	0.5735	0.11	0.06
	w 9	0,1830	0.22	0.04
	w 10	0.5420	0.20	0.11
	w 11	0.5855	0.07	0.04
Ia = 0.38, Ib = 0.36, Iib = 0.37				

Table 5: Assessed levels of information security for Company # 5

I	Index	$w_{i,j}$	$\lambda_{i,j}$	$\lambda_{i,j} \times w_{i,j}$
Ia	*w* 1	0,8240	0.14	0.12
	w 2	0.3460	0.38	0.13
	w 3	0.5630	0.24	0.13
	w 4	0.2660	0.24	0.06
Ib	*w* 5	0,4010	0.22	0.09
	w 6	0.4860	0.04	0.02
	w 7	0.33390	0.14	0.05
	w 8	0,6260	0.11	0.07
	w 9	0.2280	0.22	0.05
	w 10	0,6260	0.20	0.13
	w 11	0,6260	0.07	0.04
Ia = 0.44, Ib = 0.45, Iib = 0.44				