INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

TECHNIKI INFORMACYJNE
TEORIA I ZASTOSOWANIA

Wybrane problemy
Tom 4 (16)

poprzednio

ANALIZA SYSTEMOWA W FINANSACH
I ZARZĄDZANIU

Pod redakcją
Andrzeja MYŚLIŃSKIEGO

Warszawa 2014

INSTYTUT BADAŃ SYSTEMOWYCH
POLSKIEJ AKADEMII NAUK

TECHNIKI INFORMACYJNE
TEORIA I ZASTOSOWANIA

Wybrane problemy
Tom 4 (16)

poprzednio

ANALIZA SYSTEMOWA W FINANSACH I ZARZĄDZANIU

Pod redakcją
Andrzeja Myślińskiego

Warszawa 2014

Wykaz opiniodawców artykułów zamieszczonych
w niniejszym tomie:

Prof. Bernard De BAETS

Dr hab. Ewa BEDNARCZUK, prof. PAN

Dr hab. inż. Wiesław KRAJEWSKI, prof. PAN

Dr hab. inż. Andrzej MYŚLIŃSKI, prof. PAN

Dr inż. Jan W. OWSIŃSKI

Dr hab. Dominik ŚLĘZAK, prof. UW

Prof. dr hab. inż. Andrzej STRASZAK

Prof. dr hab. inż. Stanisław WALUKIEWICZ

ISBN 83-894-7555-3

ON MEASURES OF RISK RELATED TO IT SYSTEM SELECTION PROBLEM

Przemysław Pyzel

Systems Research Institute, Polish Academy of Sciences,
Ph. D. Studies, Warsaw, Poland,
`ppyzel@ibspan.waw.pl`

Abstract. This paper presents a survey of the methodologies of the risk of selection of the IT system. The main focus concerns concepts, models, and the measures of risk of software and IT system selection. Source Forge Research Data Archive is proposed as a source of historical data about IT implementations for the calculations of the probability of risk.
Keywords: risk, risk measures, selection of IT system, software selection

1 INTRODUCTION

As a result of strategic decisions modern institutions face the problem of selecting an IT system for selected areas of their business activity. The selection of an IT system is an elaborate process which typically comprises the following main elements:

a) analysis of needs and formulation of purposes to which the implementation of a new IT system should serve;
b) selection of relevant IT architecture (e.g. local or remote system, type of database, ways of communicating and integration);
c) determining of the conditions for implementation, maintenance, and the growth of the system;
d) collection of offers of IT systems (or software packages);
e) collection of offers of IT system implementations and IT systems integration;
f) IT system selection;
g) vendor/integrator selection and the clarification of terms of the agreement.

To a large extent, successful selection of the IT system depends on the proper realization regarding the aforementioned elements and skills of assessment of purchased IT system in terms of benefits, costs and risks. In the process of selection of the IT system risks are associated with the possibility of obstacles or errors. Usually, obstacles are related to exceeding the budget or the time and errors are related to lack of expected functionality or expected quality. Risk management takes place throughout the process of selection, purchase and implementation of the IT system. The process of risk management during the implementation of the IT system consists of periodically repeated operations, such as identification, evaluation, registration, prevention, response, monitoring. In this paper we present basic methods of determining risks related to IT system selection (e.g. selection of architecture, ways of communicating, software, implementation, vendor, integrator) also taking into account future risks of implementation and performance. The focus is on identifying and assessing risks which, in practical terms, provide the information needed to make a decision of selecting IT system. We omit further steps of risk management as logging, prevention, response, monitoring as irrelevant to the IT system selection phase.

The organization of the paper is as follows. In Section 2 we present various definitions of risks as appear in the literature. In Section 3 we present formal optimization model of IT system selection problem. In Section 4 we discuss criteria and possible applicability of various risk measures to the formal model of Section 3.

It is worth noticing that the *risk* is an independent third criterion in our model supporting the selection of the IT system (Section 3). The remaining two criteria: quality and costs were discussed in details in the previous works of the author [22–24]. Below by IT systems we mean integrated information systems (IIS).

2 RISK

2.1 Descriptive definitions of risk

In the literature concerning the IT project management and the project management methodologies, the reader is confronted with the following descriptive definitions of risk:

- Risk implies a potential, undesired event which may result in not achieving project goals [30];
- Risk is "objectified uncertainty as to the occurrence of an undesired end" [34];
- Risk implies the possibility of incurring losses, a measure of the probability of an unsatisfactory outcome, affecting the project, process or product [29];

- Risk is an uncertain event, if it were to occur would have a negative or a positive impact on achieving project objectives [20];
- Risk is the “uncertainties of results” [18];
- Risk is a function of the following attributes: events, (risk factors), the probability of their occurrence and the financial consequences that may occur as a result of events [5].

2.2 Risk detection methods, categorization of risks and risk assessment methods

The process of risk management in implementation of IIS generally consists of planning and periodically repeated operations, such as identification, registration, evaluation, prevention, response, monitoring. As noted in the introduction, at the IT system selection phase, it is necessary to perform an individual identification of risks and to assess them, which provides the information needed to select an IT system.

The most commonly used methods of risk identification are various analysis: analysis of documentation, analysis of reasons, analysis of susceptibility, SWOT analysis (strengths, weaknesses, opportunities, and threats); checklists; brainstorms; expert surveys [3], [10], [13], [16], [17], [20], [30], [35]. A detailed list of the methods described by various authors is presented in Table 1. Mark “+” means that method is explained in given source text, mark “-” means that method is not described in given text. Qualitative methods are performed by subjective experts and as a result provide verbal evaluation while quantitative methods provide objective assessments expressed numerically.

The identified project risks arranged by category are comonly shown on a hierarchically organised structure called Risk Breakdown Structure. An example of Risk Breakdown Structure by the PMBoK is shown in Fig. 1. There are many sources from which project risk may arise hence different Risk Breakdown Structure will be appropriate for different types of projects and organizations. Based on [1], some possible risk factors that should be considered at the IIS selection phase are as follows:

- Is the company well established?
- What is the longevity of the company?
- Is there support (training, developer, etc.) offered?
- Is your vendor flexible enough to make changes in the middle of development?
- Is the vendor financially stable?
- How mature is the used technology?
- How often will updates be required?

Table 1. Methods for detection of risks, categorization of risks and risk assessment methods in literature

Literature	Methods for detection of risks	Categorization of risk	Qualitative methods	Quantitative methods
[35]	brainstorm, catastrophic scenarios, analysis of the causes	+	+	-
[10]	analysis, checklists	+	+	-
[17]	brainstorm, vulnerability analysis, overview of resources	+	+	+
[30]	brainstorm, checklists	+	+	+
[13]	checklists, brainstorm, taxonomy and hierarchy, expert survey, SWOT analysis	+	+	+
[16]	survey, inspection questions	+	+	-
[3]	analysis	+	+	+
[20]	documentation reviews, information gathering techniques, checklist analysis, Assumptions analysis, SWOT analysis, expert judgment	+	+	-

Among the risk factors reported by various authors, the following factors may be listed at the IIS selection phase:

1. incomplete functionality (e.g. the declared capabilities of the software may be in the production phase or test phase);
2. incomplete integration with other software (for example, for technological reasons);
3. limitation of software license (e.g. the lack of freedom to use the system);
4. conditions for further service.

At the IIS selection phase, it is a common practice to omit an objective and numerical assessment of the risk of each option and to determine only the relative differences of the subjectively assessed risk of different options. The subjective assessment of risk is performed by an expert with extensive experience or by a team of experts [16]. Collected evaluations are often presented in the risk matrix [30]. An example of the risk matrix is shown in Table 2 [18].

Although in practice the adoption of measures of risk as estimated in Table 2 is sufficient [30], [16], in more complex situations, numerical values can also be calculated. In order to determine the level of risk of a particular event, the cost model (1) is used. Methods such as: network analysis, event tree, checklists, point methods in the quantitative analysis, and expert methods are used to determine the risk of the whole project [30].

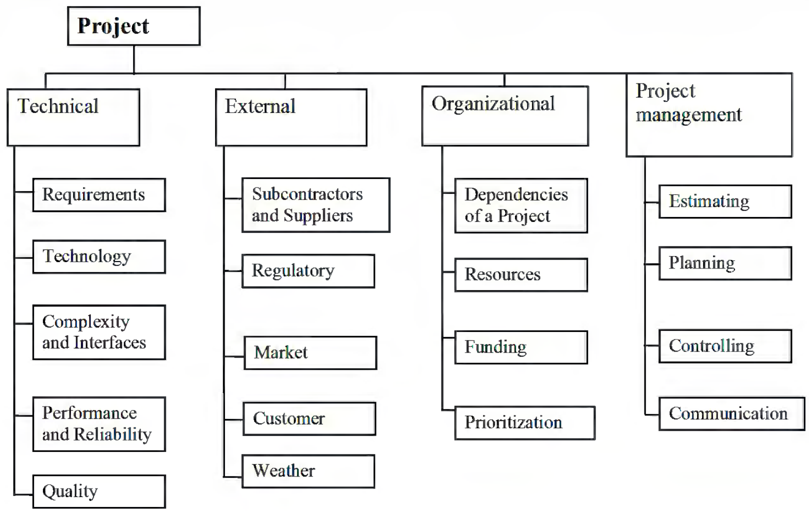

Fig. 1. Example of Risk Breakdown Structure according to PMBoK [20]

Table 2. An example of the total risk profile by PRINCE2 [18]

Probability	High	Risk No 1		
	Medium	Risk No2, No5	Risk No 7	Risk No 3
	Small	Risk No 4	Risk No 6	
		Weak	Moderate	Large
		Impact		

2.3 Quantitative risk measures

In addition to the descriptive definitions presented in the course of the paper, there exist many quantitative definitions of risk. For the purpose of this paper, only two of them will be mentioned, namely, the cost model and the value-at risk model. The cost model is the simplest method of risk evaluation which includes quantitative elements. In the cost model, the level of risk is defined as the product of the probability of an accident (undesired event) and expected loss caused by the accident (undesired event) [30]:

$$S = p * K, \tag{1}$$

where: S - risk; p - probability of an accident occurring; K - the value of potential losses in the case of an accident.

Another method which is free from the defects of subjective expert assessment is the assessment method of quantitative value associated with the risk, based on the concept of Value at Risk (VaR) [11]. Value at Risk (VaR) is widely used in business and finance, and it is a standard practice in banking supervision. In the case of application of quantitative risk assessment of IT projects, this measure also requires historical data to be taken into account, and can be used at any phase of the project, including the IIS selection phase. Value at Risk (VaR) is defined as the maximal loss that can occur in standard situations (without occurrence of unexpected factors), with a certain probability α, in a given period of time. Formally, VaR is defined by the following formula:

$$P(W \leq W_0 - VaR) = \alpha, \tag{2}$$

where: W_0 - is current value of the project (portfolio, product, financial instrument), W - is value of the project (portfolio, product, financial instrument) at the end of the given period (random variable) and α - is given level of tolerance.

After denoting the quantile of distribution corresponding to a given probability by W_α we obtain:

$$VaR = W_0 - W_\alpha. \tag{3}$$

Under the assumption that the probability of distribution is normal, VaR is defined in [11], [14].

In the case of IT projects, one of the factors generally affecting the cost is the workload. Based on historical data, it is possible to determine the rate of growth and the volatility of workload for each category of project tasks. The following methods are often used for the purpose of estimating Value at Risk (VaR) [14]:

- simulation based on historical data,
- Monte Carlo simulation,
- variance-covariance method,
- determination of any distribution quantile,
- the use of extreme value theory,
- the use of the values in the tail of the distribution.

Examples of methods for estimating VaR with the limitations and applications are presented in Table 3.

The most important advantages of the VaR method is its universality, ease of interpretation of the results, the possibility of application to determine the collateral of the capital and the application involving the asset portfolio. The disadvantages may include the limitation of use that pertain

Table 3. Exemplary methods used for quantitative risk assessment

Method	Sample distribution	Application
Monte Carlo simulation	specified theoretical distribution	at limited availability of data
Extreme value theory	other than the normal, the incidence of "fat tails"	in unusual situations
variance-covariance	multivariate normal	for a single risk or the whole portfolio

only to "normal" conditions, as well as the difficulty of estimating in the case of complex portfolios, and the sensitivity of the outcome with respect to the method of estimation.

3 THE FORMAL MODEL

One of the most important systems in any organization is the management system. For the efficient management of organizations a system is needed that combines elements of management, enables the flow, storage, and processing of information. These tasks are fulfilled by the information system. A part of the information system is a computer-based information system, which consists of hardware, software, databases, models, knowledge, and telecommunication. Integrated information system (IIS) is a computer-based information system composed of various subsystems that, as a result of integration, form a single system aiming at a particular purpose. The idea of the integration of systems is to put them together, so that by working within the whole framework, they will reinforce their efficacy [19]. Integration consists of adapting of modules to each other and merging them into one system. The integration results in high frequency and high intensity of subsystems linkages [27]. Integrated information systems are modularly structured, and support a relatively large number, if not all, areas of management [36]. IIS, through common or related databases, integrate data from various sources in order to provide timely information necessary for making management decisions. In IIS, data entered in one module of the system are readily available in other modules. Cutting-edge integrated systems ERP II (Enterprise Resource Planning II), in addition to comprehensive business support organizations, also have the ability to work with other systems over the Internet [16].

In Fig. 2 we show an example of an IIS consisting of interconnected modules (FI - finance and accounting, TR - treasure and communication with banks, CO - controlling, SD - sales, MM - materials management, RE

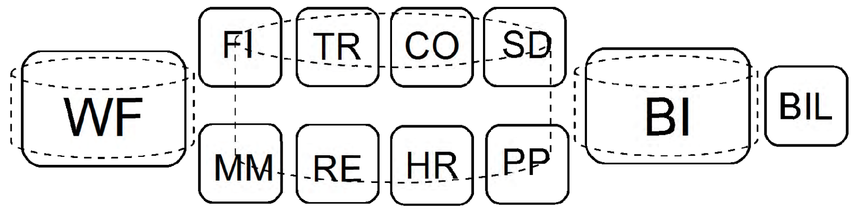

Fig. 2. An example of the IIS

- real estate, HR - human capital management, PP - production planning) and three additional systems (WF - workflow and BI - business intelligence, BIL - billing).

3.1 Building an IIS

The modules of the IIS do not need to come from the same producer, provided they use the same database or communicate with each other using standardized communication protocols and exchange data using a standardized data exchange formats. Before choosing the components to build an IIS, offers from suppliers must be collected and the costs, quality, and risks for all offers must be estimated. Software selection is a process so complicated that it is reasonable to support this process by means of optimization. Hence, there are many mathematical models that support the decision-making process. Figure 3 shows a situation in which offers are collected from various suppliers for each module of the IIS. The assessment is carried out at the level of the offered products. For each module you can only select one product from among all the ones offered. The use of such an approach results in constraints specific to the multiple-choice knapsack problem.

3.2 Optimization model of software selection

In relation to the software selection, in the literature there are various heuristic models, such as sheets of decision analysis, evaluation by a team of experts and pilot testing [1], [8]. Formal models using genetic algorithms are described in [15], [31]. There exists also a model of software selection as a single objective multiple-choice knapsack problem [9].

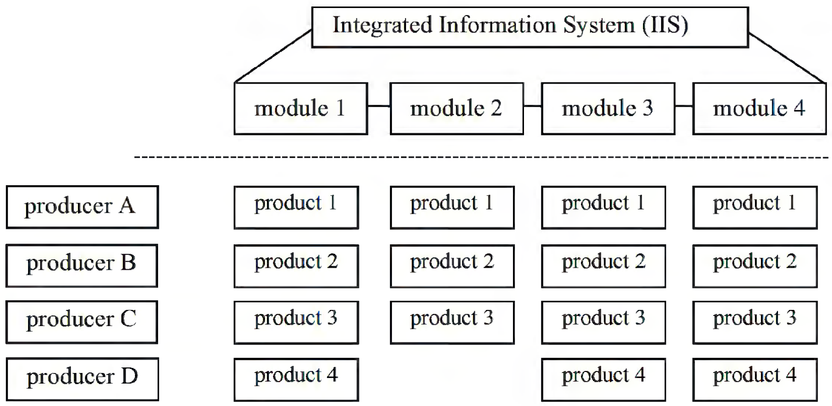

Fig. 3. Modules planned to be built in the IIS and offers presented by suppliers.

For the purpose of architectural issues (Fig. 3), the following notation is used:

m - number of modules that support the system,
n_i - number of alternative products for module i, $i = 1, ..., m$,
q_{ij} - quality level of product j for module i, $j = 1, ..., n_i$, $i = 1, ..., m$,
c_{ij} - cost of product j for module i, $j = 1, ..., n_i$, $i = 1, ..., m$,
r_{ij} - risk of product j for module i, $j = 1, ..., n_i$, $i = 1, ..., m$,
x_{ij} - decision variables of the model, $j = 1, ..., n_i$, $i = 1, ..., m$,

$$x_{ij} = \begin{cases} 1 \text{ if item } j \text{ from set } i \text{ is chosen} \\ 0 \text{ otherwise} \end{cases} \tag{4}$$

It is assumed that the criteria of quality Q, cost C and risk R are linear functions that are maximized or minimized:

1. Quality Q:

$$\max\ Q = \sum_{i=1}^{m} \sum_{j=1}^{n_i} q_{ij} x_{ij} \tag{5}$$

2. Cost C:

$$\min\ C = \sum_{i=1}^{m} \sum_{j=1}^{n_i} c_{ij} x_{ij} \tag{6}$$

3. Risk R:

$$\min\ R = \sum_{i=1}^{m} \sum_{j=1}^{n_i} r_{ij} x_{ij} \tag{7}$$

subject to:

$$\sum_{j=1}^{n_i} x_{ij} = 1,\ \ x_{ij} \in \{0,1\},\ \ i = 1,...,m,\ \ j = 1,...,n_i \tag{8}$$

The adopted constraints mean that for every unit $i = 1,...,m$ selection must be made of exactly one of the offered products $j = 1,...,n_i$. By shifting the criteria of cost and risk to the constraints we obtain the following model:

$$Q = \sum_{i=1}^{m} \sum_{j=1}^{n_i} q_{ij} x_{ij}\ \rightarrow\ \max \tag{9}$$

subject to:

$$C_B \geq \sum_{i=1}^{m} \sum_{j=1}^{n_i} c_{ij} x_{ij}\ \ \rightarrow\ \text{no more than a given budget } C_B \tag{10}$$

$$R_L \geq \sum_{i=1}^{m} \sum_{j=1}^{n_i} r_{ij} x_{ij}\ \ \rightarrow\ \text{no more than a given risk level } R_L \tag{11}$$

$$\sum_{j=1}^{n_i} x_{ij} = 1,\ \ x_{ij} = \{0,1\}\ \forall\, i,j \tag{12}$$

The model, which includes possible relationships between alternative components of modules, has been proposed in [31]. It takes into account the compatibility of component elements. This leads to the occurrence of nonlinear constraints, and consequently the nonlinear model, which may cause computational difficulties.

4 DISCUSSION OF CRITERIA AND POSSIBLE APPLICABILITY OF VARIOUS RISK MEASURES

In order to enable calculations using model given in Section 3 all criteria, i.e., quality, cost, risk, must be prepared in numerical form.

4.1 Quality

In order to assess a given option of building the IIS, one should have appropriate instruments for this purpose [25]. Sources such as the work of [12, 28, 37], legislative acts [32, 33], standards [7, 6, 21], pay attention to a number of aspects of the effectiveness of ISS, relating to: the benefits, performance, quality, or safety. Detailed analysis of these sources, allows proposing a two-level hierarchical structure of the independent characteristics and indicators [26]. In case of additional, specific requirements in a given situation, the list of characteristics can be modified. The overall assessment of the quality of the product is calculated as the weighted sum of ratings for individual characteristics which consist of the sum of the weighted ratings of appropriate indicators (according to the hierarchical structure). Weights for indicators and characteristics can be determined by experts or calculated by the decision-makers themselves, for example, by the AHP method [24].

4.2 Cost

In connection with purchase, performance and development of IIS, the following costs may be incurred [2]:

- the costs of consultation and analysis,
- the cost of software: ready packages, custom software, design tools etc.,
- equipment costs,
- installation costs: data entry, data conversion, etc.,
- environmental costs: wiring, equipment, air conditioning, etc.,
- operating costs: the cost of electricity, communication, etc.,
- costs of hardware and software maintenance,
- security costs, risk management and disaster recovery mechanisms,
- network costs: network equipment, software and maintenance,
- training costs,
- organizational costs: a new structure, a different way of managing etc.

There are also more detailed classifications of costs related to IT systems. For example, the TCO methodology provides a costs classification system and further reference statistics database of the costs of computing for many industries. A detailed classification of the areas that generate costs related to the IT systems, based on TCO and developed by IT-Investment, is presented in [4]. Not all of these costs will occur in a given organization, but each organization can use this list to create its own classification tailored to its specific situation.

4.3 Risk

Although risk can be sometimes presented in the same units as cost, like for instance VaR, it is not the same as cost. Risk may become a cost in some cases of risk management, e.g. buying the insurance.

Optimization model given in Section 3 requires that quality and cost and risk are prepared in numerical form. Therefore some qualitative methods given in Section 2 may be inadequate.

In order to move away from the subjective manner of assigning the probabilities of risk, which is popular in IT projects management, it is important to have access to the database of historical data. This can be the database containing self-collected data or an external database. The selection of an appropriate data sample as the basis for calculation (e.g. in terms of the size of the IT system, the amount of people involved in the project) is important for the particular research case. Some organizations, such as CERT Polska, Fire Brigade, Police, collect data for statistical purposes. However, the selection of an adequate data sample from these sources seems to be difficult [17]. An alternative possibility is offered by the external base SRDA (Source Forge Research Data Archive), available at sourceforge.net platform. SRDA contains a data repository of over 380 thousands of projects and can be used free of charge for scientific purposes [11].

Unfortunately, not in every situation it is possible to find historical data that are corresponding to actual situation. Sometimes for practical reasons it is better to apply expert methods, however, in that case the assesment of risk must be expressed numerically.

5 SUMMARY

The paper presented a number of approaches concerning the quantitative and qualitative assessment of risk of the IIS selection. There are some sources of historical data that can serve as the basis for the calculation and presentation of the numerical risk assessment of the IIS selection. The various approaches presented in the course of the paper will be used to the construction and analysis of formal models relating to the selection of IIS.

References

1. Bandor M.S., (2006) *Quantitative Methods for Software Selection and Evaluation*, The Software Engineering Institute, Carnegie Mellon University, (online) homepage: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=7949 (date of access: 2014-07-06).

2. Beynon-Davies P., (1999) *Inżynieria systemów informacyjnych*, p. 347, WNT, Warszawa.
3. Damodaran A., (2009) *Ryzyko strategiczne. Podstawy zarządzania ryzykiem*, Wharton School Publishing - Koźmiński Przedsiębiorczość i Zarządzanie, Warszawa.
4. Dudycz H., Dyczkowski M., (2006) *Efektywność przedsięwzięć informatycznych. Podstawy metodyczne i przykłady zastosowań*, Wydawnictwo Akademii Ekonomicznej im. Oskara Langego, Wrocław.
5. Frączkowski K., (2003) *Zarządzanie projektem informatycznym*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław.
6. International Organization for Standardization, *ISO/IEC 25010:2011 Systems and software engineering - Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models*, (online) homepage: www.iso.org
7. ISACA, *COBIT*, (online) homepage: www.isaca.org/cobit (date of access: 2014-07-06).
8. Jadhav A.S., Sonar R.M., (2009) Evaluating and selecting software packages: A review, *Information and Software Technology*, 51, 555-563.
9. Jung H.W., Byoungju C., (1999) Optimization models for quality and cost of modular software systems, *European Journal of Operational Research*, 112, 613-619.
10. Kaczmarek T.T., (2008) *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa.
11. Kieruzel M., (2012) *Metoda wartościowej oceny ryzyka projektów informatycznych*, Doctoral Thesis, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Szczecin.
12. Kisielnicki J., Sroka H., (2001) *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Agencja Wydawnicza Placet, Warszawa.
13. Korczowski A., (2010) *Zarządzanie ryzykiem w projektach informatycznych. Teoria i praktyka*, Wydawnictwo Helion (one press), Gliwice.
14. Kuziak K., (2003) *Koncepcja wartości zagrożonej*, StatSoft, (online) homepage: www.statsoft.pl/czytelnia/finanse/pdf/kuziak.pdf (date of access: 2014-07-06).
15. Kwong C.K., Mu L.F., Tang J.F., Luo X.G., (2010) Optimization of software components selection for component-based software system development, *Computers & Industrial Engineering*, 58, 618-624.
16. Lech P., (2007) *Metodyka ekonomicznej oceny przedsięwzięć informatycznych wspomagających zarządzanie organizacją*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk.
17. Liderman K., (2008) *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN SA, Warszawa.
18. Office of Government Commerce (at present: Cabinet Office, part of HM Government), 2009 *PRINCE2*, The Stationery Office, London.
19. Parys T., (1998) MRP II przykładem systemu zintegrowanego, *Informatyka*, Issue 9/98.
20. PMI, *PMBoK Guide (A Guide to the Project Management Body of Knowledge)*, Project Management Institute.
21. Polski Komitet Normalizacyjny, (2007) *PN-ISO/IEC 27001:2007*.
22. Pyzel P., (2006) Ocena efektywności zintegrowanego systemu zarządzania, *Analiza systemowa w finansach i zarządzaniu. Wybrane problemy*, Vol. 8, Red. Hołubiec J., Instytut Badań Systemowych PAN, Warszawa.
23. Pyzel P., (2007) *Modeling IMS Efficiency on the Base of Expert Knowledge*. Presentation at the conference PD FCCS 2007, www.fccs.swspiz.pl/fccs2007/index.html
24. Pyzel P., (2009) Zastosowanie metody AHP do oceny efektywności działania zintegrowanego systemu zarządzania, *Analiza systemowa w finansach i zarządzaniu. Wybrane problemy*. Vol. 11, Red. Hołubiec J., Instytut Badań Systemowych PAN, Warszawa.
25. Pyzel P., (2010) O problemie oceny efektywności systemów informatycznych, *Analiza systemowa w finansach i zarządzaniu. Wybrane problemy*. Vol. 12, Red. Hołubiec J., Instytut Badań Systemowych PAN, Warszawa.

26. Pyzel P., (2012) Propozycja metody oceny efektywności systemów MIS, *Techniki informacyjne - teoria i zastosowania*. Vol. 2 (14). Red. Myśliński A., Instytut Badań Systemowych PAN, Warszawa.
27. Santarek K., (1995) Computer Integrated Manufacturing, *CIM-ARIS Computer Integrated Information Systems*, Red. Kasprzak T.
28. Sienkiewicz P., (1987) *Teoria efektywności systemów*, Zakład Narodowy im. Ossolińskich - Wydawnictwo, Wrocław.
29. Software Engineering Institute, *Capability Maturity Models*, Carnegie Mellon University.
30. Szyjewski Z., (2001) *Zarządzanie Projektami Informatycznymi. Metodyka Tworzenia Systemów Informatycznych*, Placet, Warszawa.
31. Tang J.F., Mu L.F., Kwong C.K., Luo X.G., (2011) An optimization model for software component selection under multiple applications development, *European Journal of Operational Research*, 212, 301-311.
32. *Ustawa z dn. 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2002 r. Nr 101 poz 926*, and *Rozporządzenie Min. Spraw Wewn. i Adm. z dn. 29 kwietnia 2004 r. (), Dz. U. z dn. 1 maja 2004 r.*
33. *Ustawa z dnia 29 września 1994 r. o rachunkowości, Dz.U. 1994 Nr 121 poz. 591.*
34. Woodward M.R., Hennell M.A., Hedley, (1979) A Measure of Control Flow Complexity in Program Text, *IEEE Transactions on Software Engineering*, Vol. 5.
35. Wróblewski P., (2005) *Zarządzanie projektami informatycznymi dla praktyków*, Wydawnictwo Helion, Gliwice.
36. Wrycza S., (2010) *Informatyka ekonomiczna*, PWE, Warszawa.
37. Zalewski A., Cegieła R., Sacha K., *Modele i praktyka audytu informatycznego*, (online) homepage: www.e-informatyka.pl/wiki/Modele_i_praktyka_audytu_informatycznego (date of access: 2014-07-06).

O MIARACH RYZYKA ZWIĄZANEGO Z WYBOREM SYSTEMU IT

Streszczenie. W artykule przedstawiono przegląd metod oceny ryzyka wyboru systemu informatycznego. Omówiono pojęcia, modele i miary ryzyka związanego z wyborem oprogramowania i systemu informatycznego.
Wskazano bazę danych o historii realizacji projektów informatycznych SRDA, która może być źrodłem danych do obliczeń prawdopodobieństwa wystąpienia określonego ryzyka.
Słowa kluczowe: ryzyko, miary ryzyka, selekcja kryteriów IT, wybór oprogramowania

ISBN 83-894-7555-3