THE EFFECTIVENESS AND SECURITY OF MANAGEMENT SUPPORT INFORMATION SYSTEMS

Hubert Szczepaniuk, Piotr Zaskórski

Military University of Technology

Abstract. Efficient management of the organization, especially in threat and crisis conditions, implies the need to assess both the effectiveness and security of information systems, including computer information systems. The assessment of safety and effectiveness level of management support systems could become the base for determining the directions and methods of improving the management of any organization. Identifying the sources of threats and reductions in the system effectiveness can be an indication for the effective implementation of IT in the organization. In this article the author's intention is to present a safety dilemma and the effectiveness of the management support information systems with particular emphasis on risk management project. Focus is made on the following issues: the notion of MSIS (Management Support Information Systems), the analysis of chosen IMIS (Integrated Management Information Systems), measures and models of system effectiveness assessment, MSIS security as the determinant of effectiveness, modeling the assessment of IMIS effectiveness. Proposed measures and model for measurement of the system features is therefore described.

1. INTRODUCTION

The ability to effectively acquire, define and analyze the facts and events that are converted into knowledge, which is a tool for effective management, is becoming a necessity in modern organizations. Such mechanisms are provided by modern information systems [7].

In many organizations that operate in strong temporal conditions, an efficient, safe and effective information system is acquiring a fundamental significance [12]. Efficient management of the organization, especially in threat and crisis conditions, implies the need to assess both the effectiveness and security of information systems, including computer information systems. The assessment of safety and effectiveness level of management support systems could become the base for determining the directions and methods of improving the management of any organization. Information security is one of the main components of security of the whole organization. Identifying the sources of threats and reductions in the system effectiveness can be an indication for the effective implementation of IT in the organization, inter alia, by using system patterns [10] in the form of management support information systems (MSIS). The security level of

management information system could also become a good indicator for measuring the generic and overall effectiveness [1] of design and implementation projects.

2. THE NOTION OF MSIS

The management information system is a part of the information system implemented by means of computer technology, the aim of which is to support the processes of planning, standardization, inventory, control and assessment of events in the organization. An efficient management support information system should carry put the functions in acquisition, collection, processing and sharing of information [11]. Implementation of MSIS in the organization often causes structural changes and improves potential of the organization, but it is also connected with considerable financial and organizational expenditure. The decision to implement CMMS in the organization is characterized by a high risk of failure. The implementation of CMMS may lead to failure, manifested by not achieving the assumed functionality and/or exceeding the assumed time and implementation costs – such failure may cause negative effects in the functioning of the organization.

When choosing MSIS, the assumed systems should not always be implemented. The pursuit of complexity is a natural feature of information and decision-making processes. However, the simpler solutions, which are cheaper in implementation and easier to use, are often sufficient. MSIS constitute a very numerous set of objects and an appropriate choice of solutions relevant to the needs is faced with the difficulty manifested by distinguishing a subset of systems that have common and complementary features compared to other systems [9]. There are many divisions of MSIS according to the established criteria. One of them is the division proposed by J. Kisieliński [3] into three fundamental generations, according to the criterion of the information needs of decision makers:

- Generation I – transaction systems – they do not require specialist equipment or software. They support the organization in carrying out the following functions: accounting, personnel management, logistics, etc. In practice, most systems supporting the management are the systems of this generation.
- Generation II – systems for informing the management – systems using a database, allowing to operate in request – response mode. The use of database technology has lead to creation of Management Information Systems (MIS) and Integrated Management Information Systems (IMIS). Systems of class MPR II, ERP, ERP II, CRM and SCM are the contemporary generation of IMIS.
- Generation III – advisory systems – the most complex and very dynamically developing during the recent years. A particular feature of these systems is the use of databases and data warehouses, model bases, as well as artificial

intelligence and knowledge bases. Tools such as OLAP and technologies of data mining/"exploring" are also used. In this generation of systems, the following division can be used: Decision Support Systems, Expert Systems and Artificial Intelligence Systems.

Other divisions of information systems, presented in the literature on the subject, assume the functions performed by this system as the main criterion. The literature distinguishes the systems of: registration, planning, human resources management, information systems for marketing, production, etc. In general, these systems can be passive or active, and they support the processes of the organization management.

3. THE ANALYSIS OF CHOSEN IMIS

Observation of the MCMS development indicates a tendency to create integrated management information systems (IMIS) that connect the abovementioned generations. Integrated systems support all the basic functions of management in the organization through modules designed to handle various processes of processing data in the organization. The tendency to integrate systems began in the nineties of the 20th century – a period which was also characterized by a very rapid development of IT. The systems known as MPR II[1] (Manufacturing Resource Planning) and ERP/ERP II[2] (Enterprise Resource Planning) were created.

The standard for functions of class II MPR systems has been specified by the APICS[3] association and includes:

- business planning, production and sales planning, and scheduling of sales and production plan,
- demand management and planning of material needs,
- subsystem of product structure and subsystem of material transactions,
- subsystem of production flow and control schedule,
- planning of production capacity and management of the work area,
- supply and planning of distribution,
- workshop aids,
- interface for financial planning,
- simulations and measurement of the system activity.

[1] See: *Funkcjonalność informatycznych systemów zarządzania*, Tom I i II by A. Januszewski, WN PWN, Warszawa, 2008.

[2] Ibidem.

[3] APICS The Association for Operations Management (American Production and Inventory Control Society) – a non-profit organization dealing with standardization of production control methods, known as MRP i MRPII.

As can be seen, IMIS to a great extent integrates people, data, knowledge and processes in the organization. The concept of product in these systems is universal and can also concern some services or even projects.

ERP class systems enrich MRP II with financial procedures based on economic calculation (e.g. cost account, management accounting, etc.). Systems of this class are currently the most complex class of integrated management systems[4]. Thanks to the enrichment with financial procedures, the control of production/service process is possible, also according to the quantity and value criteria. ERP class systems are being subject to a dynamic and gradual evolution of technology used in them[5]. An important step in the technical evolution of ERP systems are:

- transition to component architecture, enabling any construction of system based on the user's needs and the scope of the organization's activities,
- pre-configured modules of the system, which reduces the implementation time,
- the use of multimedia technologies,
- adapting to Windows environment in order to increase the number of system users,
- replacing GUI with a web browser, which forces the adaptation to HTTP standards,
- the use of Internet network services (Web Services) to exchange data with the environment,
- the use of XML to exchange electronic documents,
- integration of OLAP analytical tools and data mining into ERP packages,
- openness to integration with CAD/CAM and GIS (Geographical Information System) environments, and the use of mobile technologies,
- openness to integration of system components that come from different suppliers by using COM and CORBA standards[6].

Analysis of chosen IMIS classes shows that many solutions can be implemented and used both in the business structures, as well as in the structures of public administration. This means their complex nature enables the integration of information resources, but causes risks connected to the integrity, confidentiality and access.

[4] Unfortunately, there is currently no formal description of the functions issued by APIS for the systems of this class. Nonetheless, the dynamic development of these systems is ongoing.

[5] The first ERP systems were constructed, inter alia, from the following components: relational database equipped in a structural query language (SQL) and fourth-generation programming language (4GL), a graphical user interface (GUI), the work based on the model of client/server communication, providing API standards to the programmers, dedicated client software and the implementation of EDI standard.

[6] See: Wikipedia www.wikipedia.org (of 20.03.2010).

4. MEASURES AND MODELS OF SYSTEM EFFECTIVENESS ASSESSMENT

Considering the question of MSIS effectiveness [1], there are various criteria that should be specified, in respect of which the effectiveness of such systems can be studied [11]. Thus, there are the following types of MSIS effectiveness criteria:

- *operational criteria* – a system feature, expressing the ability of the system to perform activity that enables to carry out the final purpose,
- *economic criteria* – effectiveness assessment, carried out using economic calculation; it is based on the relationship that occurs between expenses incurred for IT and results obtained as a result of its use,
- *information criteria* – determine the so-called information performance. The features tested in this context are: comprehensibility, reliability and update of information, the degree of information processing and time of information flow,
- *technical criteria* – determine the effectiveness of the system components (reliability, readiness and durability),
- *operating criteria* – represent the influence of functioning of individual system components on the ability of the system to operate efficiently.

The economic effectiveness is usually defined as the outcome of action taken, described as the relationship between obtained results and incurred expenditure. The most general measure of MSIS use effectiveness is *return of investment* (ROI):

ROI = RESULTS / EXPENDITURE

The overall calculation above can answer the question whether the chosen option of the use of IT/IS solution will be a viable solution[7]. The so-called *relative effectiveness factor* can be another useful measure:

$$K = \frac{\Delta E}{\Delta I},$$

where:

K – relative effectiveness factor,

ΔE – increase in effect caused by the use of MSIS,

ΔI – increase in expenditures caused by the use of MSIS[8] .

If there is a congregation of different possible options for investing in MSIS, then the above indicator allows to answer the question which of the options is most beneficial. Apart from individual economic indicators, the assessment

[7] It is worth noting that the level of security of resources and the whole system can be the measure of performance.

[8] Increase in expenditures directly associated with safety improvement/risk reduction, including the effects of threats.

of economic effectiveness of MSIS can also use the so-called system methods, which generally do not rely solely on the financial value criterion, but on more general criteria that may be related to strategies or needs of the organization. In this way, it is possible to use a system assessment of the object from the moment of intending to introduce changes to the moment of payoff. The outline of procedures used in the method of system calculation of effectiveness is associated with various stages, including:

- preliminary stage – identifying the problem and collecting the necessary data,
- the stage of formulating the problem and determining the options for implementation,
- analysis and selection of methods adequate for determining the effectiveness of IT use in the organization and their validation,
- verification of acquired decisions.

One of the key elements of the procedure is constructing the matrix of decision-making situations (Figure 1). The elements of this matrix are the individual actions and the subsequent levels of decision-making, related to the choice of solutions. Of course, the included parameters of choice are used as examples, but give a picture of multi-dimensionality of choosing specific tools for supporting management and improvement of the organization.

No.	Decision-making level	Characteristics of individual actions				
1	For what purpose will the informatization be implemented?	Supply	Production	Market	…	Personnel
2	What operating system will be used?	OS/2	DOS	Windows 7	…	Linux
3	What application software will be used?	Ingres	Progres	MS Word	…	MS Office
4	….	…	…	…	…	….

Figure 1. An example fragment of decision-making matrix9
Source: own elaboration based on [5]

Methods and techniques for evaluating the system effectiveness are inextricably related to the area of risk assessment and security of the whole organization [8] in

[9] The decision-making matrix can become a basis for preliminary assessment of implementation effectiveness of IT/IS and the indication for target decisions in terms of usability, functionality, reliability and efficiency of solutions, also in relation to the level of risk and associated security.

the context of information resources, which are an important element of critical infrastructure of the organization.

5. MSIS SECURITY AS THE DETERMINANT OF EFFECTIVENESS

MSIS ensures the exchange of information with different levels of confidentiality, which enforces the use of a range of solutions determining the security of information resources of the organization[10], in terms of:

- verification of user identity,
- control of user access,
- implementation of obligatory rules of conduct,
- ensuring an appropriate level of security for storing and transmitting information.

In order to ensure the efficient operation of MSIS in the organization, the guarantee of security requirements for information resources of the organization becomes a priority[11], including:

- securing information technology equipment against damage and accidents,
- public keys for cryptographic communication,
- management measures used to protect, detect and respond to events,
- firewall hardware and software,
- specially designed hardware and software of operating systems in trusted technology.

Security of the organization can be treated as a complement of the normalized risk measure. Information security is an important element of overall system security, as mentioned above. Currently, MSIS class systems (including IMIS) are an integral part of management. Hence, their level of security can be the basis for assessing the effectiveness of activities, especially in critical situations. There has always been, there is, and there will always be risk in an everyday life of every human being, therefore it is also present in the implementation of management processes, including information and decision-making processes. The results of any processes arise form the risks involved[12], which is reflected by the process deviations from the model, according to various aspects of assessment (see table below):

[10] *Zasoby informacyjne komponentem infrastruktury krytycznej organizacji*, V Międzynarodowa Konferencja Naukowa *Katastrofy Naturalne i Cywilizacyjne. ZAGROŻENIA I WYZWANIA DLA BEZPIECZEŃSTWA* by P. Zaskórski, Wrocław-Bełchatów 3-5/06/2009.

[11] Ibidem.

[12] The Internet: www.pwsz.nysa.pl/instytut/finanse/wilimowska, May 2010.

Groups of risk definition	
The category of decisions taken to achieve specific purposes	Risk is the uncertainty associated with the future events or the results of decisions.
The source of risk	The uncertainty of information or taken decision, which is not optimal because of the assumed purpose is the source of risk.
According to the manifestation of risk	Risk is a deviation from the expected value of the assumed purpose.
Probabilistic or statistical measure	Risk is a subjective probability of one-off events or those which did not occur at all.
The theory of pattern recognition	Risk is a discrete measure using the theory of pattern recognition and the cost associated with this measure (either created, or an existing abstract models of risk can be used, and then the studied risk is put in the risk area).
Reliability theory	In this case reliability means the object property defined by its ability to meet the requirements (defects reflect the adverse events).

Types of risks arise from different sources, so they can be classified according to different criteria. Thus, the following risks can be distinguished for introduced information technologies:

- Actual, meaning the one that is analyzed basing on the law of large numbers, that is, concerning uncertain phenomena, which have known and described history – therefore they are subject to probabilistic description, e.g. natural disasters, catastrophes, equipment failures.
- Subjective, meaning the one resulting from the incompetence of the man who is conducting the analysis and making decisions.
- Objective, meaning the one resulting from the unpredictability of the future events of various nature.

Risk identification is based on defining the types of risks to which a given process exposed, and answering the question: what kind of threat concerns us? Potential risk factors may be numerous, so it is very important to detect the source that is the first cause of possible future problems.

The main task of qualitative analysis is an estimate the probability and consequences of the occurrence of previously identified threats. The result of qualitative risk analysis: an overall ranking of the process of implementation, operation and use of MSIS in terms of risk, including the hierarchy of risk list (which allows to specify the sources of risk with a very significant, potentially negative influence on the process, or possibly irrelevant to the process) and trends arising from the results of qualitative risk analysis, conducted repeatedly during the implementation of these information and decision-making processes.

The purpose of quantitative risk analysis is to determine the measurable values of the probability and consequences of adverse events, both for the individual actions of the process and for the whole enterprise. This measurement allows determining the chance of achieving objectives, specifying levels of necessary reserves and conducting a detailed "what-if" analysis, all this using measurable values. Quantitative risk analysis is often preceded by qualitative studies. Several strategies are commonly used for the process of planning the responses to risk. An appropriate action plan should be chosen for each type of risk, so that the taken action increases the level of integrity, confidentiality and selective availability of information resources:

Risk management is a process in which there is the need to monitor the level of risk and control the entire process of risk management. Risk analysis techniques include preliminary threat analysis, RISC SCORE and opinion of experts. One of the most accessible and universal methods for measuring and assessing risk is the risk indicator method. In the method, the probability of results of the event is specified and presented by the two risk parameters: exposure to risk and vulnerability of specified processes/systems to the threat and the probability of occurrence of the event, so:

$$\mathbf{Ry = S \times E \times P \times D},$$

- Ry – risk level indicator,
- S – potential effects of threat,
- E – exposure to risk,
- P – the probability of the occurrence of threat,
- D – vulnerability to threat.

Modelling the range of risk identification and, above all, identification of sources of threats and their effects is associated with:

- early awareness of potential risks, which is the basis for effective risk reduction,
- estimating the parameters that designate risk, which is always the first step in the process of risk management,
- documenting the events and effects in order to use the analogy model through clear description of the information concerning risk, such as:
- description of risk – the description of a given event that, if occurs, has a negative influence on the system resources,
- context of risk – description of the event location as part of tasks, personnel and products in information and decision-making process.

Assessment and validation of risk is a good reflection of the security level of information resources and the entire system of operation. Assessment of safety level can also constitute the measure of one of the purposes, used for assessing the effectiveness of MSIS, including IMIS.

6. MODELING THE ASSESSMENT OF IMIS EFFECTIVENESS

The difficulty of precise assessment of the effectiveness measures for the functioning of MSIS in the organization is primarily due to difficulties in estimating which part of the overall effect is a result of using MSIS, and which part of these effects is related to other operations of the organization.

The effects of information project are influenced not only by the assessment of the effects of information system in the organization itself, but also the impact of the environment (Figure 2), which is difficult to estimate. Using the notation of set theory, and assuming that the internal (C_W) and external (C_Z) partial effect has been obtained through the use of MSIS, it can be seen that the difference:

$$C_W \setminus (A_W \cap B_W \cap C_W \cap D_W \cap \dots)$$

is a clear internal effect of the organization caused by the use of MSIS.

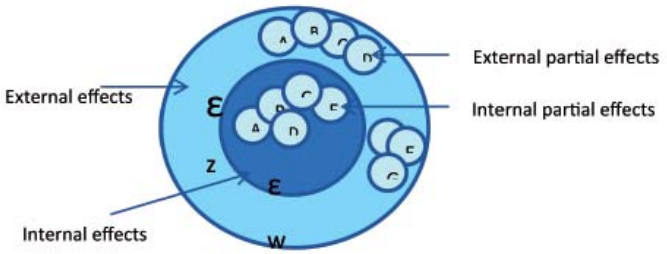

Figure 2. The effects of the organization's activity
Source: own elaboration

Difference:

$$C_Z \setminus (A_Z \cap B_Z \cap C_Z \cap D_Z \cap \dots)$$

is a *clear internal effect of the organization, caused by the use of MSIS*.

Based on previous assumptions, it is also possible to determine the summary effect of using the information system:

$$C = C_Z \cup C_W,$$

and the participation of effect obtained by using MSIS in the total effect of the organization's activity:

$$\alpha = \frac{C_z \cup C_w}{\varepsilon_w \cup \varepsilon},$$

where $\varepsilon = \varepsilon_z \cup \varepsilon_w$.

When assessing the effectiveness of MSIS, it is also important to determine the place and type of effects that have been created. By synthesizing the classification available in the literature, it is possible to enumerate the following effects of the investments in: MSIS:

- technical: increase in the speed of information transmission, ensuring confidentiality, etc.,
- economic: improvement of the results of the organization's economic activities, optimization of decisions, etc.,
- organizational: improvement of document circulation, eliminating unnecessary inventory, reorganization of processes, etc.,
- socio-psychological: the better adaptation of staff to the team, etc.

Therefore, it can be said that the effectiveness of the functioning of MSIS/IMIS should also be seen in the direct context of their security, and the measures of objectives could include the value of the system security level in relation to expenditures incurred, or their increase. Of course, this requires, above all, analysis and risk assessment.

7. CONCLUSION

In terms of measuring and assessing the effectiveness of MSIS implementation in the organization, there are many conflicting opinions, beginning from the statements that IT brings no advantages in this field to opinions about the fundamental role of this technology. Today, entire strategies for using integrated information systems are being created, changing the methods, effectiveness and scope of management [2]. Success indicator for large information technology projects implemented in organizations is rather low. There is a lack of sound and objective scientific apparatus that would evaluate the effectiveness of the implementation and use of MSIS.

It is difficult to find a common approach in the field of modelling the research and evaluating the effectiveness of MSIS in the literature on the subject. It is therefore justified to conduct research on modelling the effectiveness of MSIS. This article attempts to propose measures and a model for measurement of the system features, which affect the security of the organization and its informational effectiveness, understood as a component of the effectiveness of all activities.

BIBLIOGRAPHY

1. W.W. Bojarski, *Efektywność systemowa przedsięwzięć gospodarczych*, WSzZiP, Warszawa 2001.
2. J. Champy, *X-Engineering przedsiębiorstwa*, Agencja Wydawnicza Placet 2003.

3. A. Hamrol, W. Mantura, *Zarządzanie jakością – teoria i praktyka*, Wyd. PWN, Warszawa 2002.
4. A. Januszewski, *Funkcjonalność informatycznych systemów zarządzania*, Tom I i II, WN PWN, Warszawa 2008.
5. T.T. Kaczmarek, G. Ćwiek, *Ryzyko kryzysu a ciągłość działania. Business Continuity Management*, Difin, Warszawa 2009.
6. T. Kasprzak (red. naukowa), *Modele referencyjne w zarządzaniu procesami biznesu*, DIFIN, Warszawa 2005.
7. A. Kijewska, *Systemy informatyczne w zarządzaniu*, Wyd. Pol. Śl., Gliwice 2005.
8. J. Kisieliński, *MIS. Systemy informatyczne zarządzania*, Agencja Wydawnicza Placet, Warszawa 2009.
9. M. Trocki, B. Grucza, K. Ogonek, *Zarządzanie projektami*, PWE, Warszawa 2003.
10. P. Zaskórski, *Strategie informacyjne w zarządzaniu organizacjami gospodarczymi*, WAT, Warszawa 2005.
11. P. Zaskórski, *Zasoby informacyjne komponentem infrastruktury krytycznej organizacji*, V Międzynarodowa Konferencja Naukowa *Katastrofy Naturalne i Cywilizacyjne. ZAGROŻENIA I WYZWANIA DLA BEZPIECZEŃSTWA*, Wrocław-Bełchatów 3-5/06/2009.

Efektywność i bezpieczeństwo informatycznych systemów wspomagania zarządzania

Streszczenie. Sprawne zarządzanie organizacją, szczególnie w warunkach zagrożeń i kryzysów, implikuje potrzebę oceny zarówno efektywności jak i bezpieczeństwa systemów informacyjnych, w tym systemów informatycznych. Ocena poziomu bezpieczeństwa i efektywności systemów wspomagających zarządzanie może stać się podstawą ustalenia kierunków i metod usprawnienia zarządzania każdą organizacją. Identyfikacja źródeł zagrożeń i obniżania efektywności systemu może być wskazaniem dla efektywnego wdrożenia IT w organizacji. W referacie autorzy przedstawiają problem bezpieczeństwa i efektywności informatycznych systemów wspomagania zarządzania ze szczególnym uwzględnieniem zarządzania ryzykiem projektowym. Odnoszą się przy tym do najbardziej istotnych zagadnień: istoty ISWZ (Informatycznych Systemów Wspomagania Zarządzania), analizy wybranych ZSIZ (Zintegrowanych Systemów Wspomagania Zarządzania), miary i modele efektywności systemowej, bezpieczeństwa ISWZ jako determinantą efektywności, modelowania oceny efektywności ZSIZ. Zostaje przedstawiona również próba miar i modelu pomiaru systemu w przełożeniu na efektywność informacyjną i bezpieczeństwo.