Foundations of Management, Vol. 2, No. 2 (2010), ISSN 2080-7279
DOI: 10.2478/v10238-012-0029-4

IT SYSTEMS SECURITY MANAGEMENT IN MIGRATION PROCESS

Sylwester PIĘTA

Faculty of Management
Warsaw University of Technology, 02-524 Warszawa, Poland
e-mail: s.pieta@wz.pw.edu.pl

Abstract: This paper looks at the issue of IT systems migration as well as problems related to security policy in migration processes. Problem of migration is viewed in a broad context of changes which occur during construction or modernization of an IT system. Migration projects were classified against the background of wide spectrum of informatization strategy issues and sources of threats to information security were pointed out. Also, guidelines for improvement of security in migration process were presented.

Key words: informatization strategy, migration, migration scenario, software versioning, upgrade, source system, target system, security, system resources, data and information security, risk management, information systems protection, security policy, business continuity, system project, project management.

1 Introduction

The functioning of a modern organization encompasses, next to business strategy, informatization strategy, which should bring together both business and IT goals. It is, apart from natural systems evolution, the key factor which causes IT systems to constantly undergo changes. Sometimes, these are minor changes connected with functional development, while, some other times, a giant technological leaps of system platform and business applications. IT infrastructure, similarly to every other organizational resource, requires appropriate management and exploitation – changes disturb this process. In principle, only seldom the situation is stable in the long term, when systems can be exploited normally, in accordance with the established business goals and the introduced security policy.

IT systems security and IT systems migration are, today, two well-known areas for the managing and IT staff. They are known because of their fundamental influence on organizational development and business continuity.

Successful migration of IT system and its information surrounding into new organizational and technical conditions requires this process to be treated as an undertaking of strategic character. Therefore, it is best to prepare the migration process as well as plan and control its implementation on the basis of such best practices and management, support, maintenance and IT development models as COBIT [1], ITIL [2] or CMM/CMMi[3].

Right implementation of new information technologies enables the organization to enter into equal competitive struggle or even become the industry leader, while, on the other hand, implementation failures may become extremely costly, leading even to organization bankruptcy. It is similar in the area of security. Flaws of security policy constitute potential trouble for organization. Increased importance of electronic data processing requires taking broader protective measures towards the infrastructure used, as well as information and data themselves. One investment-stimulating factor is surely the fear of losing data, but also, for some industries, adequate law regulations and, more and more often, care for the company goodwill.

Process of IT system migration is a remarkable situation for an organization. Because of appearance of new technologies, new tasks for employees, new personnel for the organization, we deal with threats in the field covered by migration, which not only may not be included in procedures but also may not be considered at all.

[1] COBIT (Control OBjectives for Information) – coherent and clear model/set of best practices for IT management, addressed to managers, auditors and users of information technologies.

[2] ITIL® (Information Technology Infrastructure Library) – set of complex recommendations of IT industry, on the basis of chich the international norm for IT service management – ISO/IEC 20000 Service Management, was created.

[3] CMM/CMMi (Capability Maturity Model *Integration*) – general model which determines organization maturity with regard to realization of given goals and enables to improve organizational inner processes in an organized and ordered manner.

This work concentrates on describing the issue of migration and on information security in migration processes against the background of informatization strategy. Description of informatization strategy has been limited to necessary minimum. In order to present a complex approach to the problem of security, one has to speak of information security of organization. Complete security policy consists of organizational matters and information technologies both in routine utilization and in emergency situations, such as: malfunctions, crises and migrations.

1.1 Informatization strategy

Strategy is most often defined as "clearly formulated goals together with means, methods and rules of their achievement". Strategy, from the moment of their establishment, has a defined time horizon, in which it operates. Works concerning strategy improvement should be carried out continuously in such a way, that it always precedes executive projects connected with it – in this case, information system migration project.

From the informatization strategy should result the program (plan) for its realization, especially:

- assumptions, that is limitations (spatial, financial, staff, time) and target parameters (flows, capacities, performances),
- necessary information (models, methods), software (operation systems, software tools) and hardware resources,
- operations and design processes as well as project management methods (including requirements concerning flexibility and quality of solutions).

When establishing informatization strategy, one has to pay attention to:

- differentiation between IT infrastructure (hardware, software), information system (information sources, information processing procedures, organizational bylaws) and IT system (databases, software tools, application programs, procedures and methods of data processing),
- necessity to systematically identify information requirements in organizational structure and its environment,
- necessity to establish a multi-layer integrated information system model and IT system model,
- necessity to follow and analyze development plans and undertakings of competition and to gather information on IT systems and technologies.

Examples of technical and organizational undertakings, which should be included (calculated) in informatization strategy concerning the issue of IT system migration are:

- target structure and development level of an information system, part of which will be the IT system to undergo migration,
- systematic identification of information requirements of the new information system users,
- construction and development of a target IT system in an integrated architecture, which will guarantee integration of all information processes at a limited number of technological (executive) platforms.

In the IT strategies realization programs, it is advisable to pay particular attention to some groups of discrepancies, which accompany design or modernization of an integrated IT system discrepancy between:

- diversity and integration of product service processes in the IT system,
- diffusion and integration of data in the IT system databases,
- the need to modernize and the need to fulfill ad hoc functions,
- security and accessibility of IT system resources,
- current state of the IT system (before migration) and requirements set for the new system (after migration).

Minimum list of informatization program evaluation criteria:

- standard of technical and program realization of system after migration (modernity of the proposed solutions),
- operational reliability and level of system security,
- ensuring organizational business continuity during the whole migration process,
- time-schedule and costs of execution,
- increased possibility to broaden system functionality after migration,
- simplicity of system administration no lesser than before migration.

1.2 Problem of migration

A dozen or several dozen years ago there would often be a situation, when an IT system was introduced to an organization in order to support or replace manual tasks carried out by personnel. Today, it is most often a change within an already existing infrastructure. Dur-

ing the use of IT systems comes the obvious need of expanding, changing or replacing them. Each case comes with specific requirements characteristic for particular business. It should be noted, that launching a new IT system in parallel to another system, i.e. paper one, does not carry the threat of disrupting business continuity. In case of migration processes, in spite of all the preventive measures, there comes a moment when business support is switched from an appropriately working system to a new system burdened with potential errors. By maintaining for a longer period the parallel work of the old system, we do leave ourselves with a way for retreat, however, this comes with at least short stoppage and, as a rule, with costs adequate to the system "weight".

Migration means entering a path full of potential threats to business continuity and, additionally, all activities in this process, by their nature, open the possibilities of undesirable events from the point of view of security.

Expenses for a new, improved system will find justification from the point of view of management staff. However, from the economic departments' point of view, ensuring security does not result in increased sales or profit. Such investments are hard to force through in budget plans, as they do not bring measurable, easy to calculate benefits. ROSI [4] index, used in some foreign companies is, most of the time, wrongly defined if defined at all.

2 Definitions

In the beginning, a couple of definitions are presented which will become helpful in some further considerations.

- Migration

Migration[5] (lat. 'migratio' = resettlement) – 1. Journey, resettlement of people within country, 2. Active or passive resettlement of plants or animals from one area to another.

Migration with regard to IT systems refers to process of changes in an IT system, which aims at moving from a state called source system to a state called target system. Migration-related issues may consist of technological (software, hardware), organizational and legal problems.

[4] Return On Security Investment.

[5] Foreign Words Dictionary, PWN 1980, edited by Jan Tokarski.

Reasons for the migration necessity may be of various nature: from necessity to run minor system updates to issues related to merging or dividing the organization or its units. In the research [12] by DiS (Market research agency DiS) entitled "ERP systems migrations" the most often reason for migration was the necessity to broaden functionality, and the second most often was the change of company IT strategy. Changes in capital structure are considered one of the most often reasons for organizational migrations.

It is necessary to add that, in all cases, migration is connected with high expenditures, relatively high in comparison to the cost of building an IT system from scratch. Migration is most often carried out in medium and large organizations, where complexity of an IT system can be measured with the use of function point, i.e. number of entries and exits from the system, or the number of entities [15].

- Source system

In this work source system is defined as a state of an IT system, which encompasses the following resources: hardware, software, human resources, organizational procedures and information resources, before launching of migration process.

- Target environment

Target environment is defined as such a state of IT system, which encompasses the following resources: hardware, software, human resources, organizational procedures and information resources, after migration process is finished. Migration process may influence all the above mentioned resources in order to move from source system to target environment.

3 Classification of migration projects

The classification presented below has, in some aspects, an arbitrary character, which obviously, results in the fact that some elements of the defined migration types may be mixed, i.e. technical upgrade and realization of minor improvements, technical upgrade and authorization list or postponed realization. Organizational migration, on the other hand, will, in principle, be connected with a number of system upgrades. Within the classification, the reasons for launching migration projects are presented:

- upgrade
  - it is an undertaking which consists in updating the version of software used; most often, it is connected with adding new functions to the sys-

tem or removing significant errors; designations used in the system version designation scheme are mentioned in section 9.1 Versioning,
  - reasons: appearance of new version containing new functions, removal of significant errors, necessity to align the data format in the exchange with other users/systems,
- technical migration
  - project consisting of changing the system or the operational systems, hardware or access methods, when possible without introduction of any improvements to the IT system functionality,
  - reasons: appearance of new version of software which requires new resources such as operation system or hardware, routine activity consisting in periodical replacement of hardware, security measures – replacing the hardware-system platform with a safer one,
- functional migration
  - aim of this project is to implement improvements or introduce brand new functions to the system,
  - reasons: necessity to introduce new functions to the system,
- placement migration
  - alteration of functional migration; aim of this project is to introduce changes and improvements which enable use of the system by people, who use different language than the default one; in principle, this requires bigger amount of work, which is not only directed at translation, but also: user profile expansion, adding dictionaries, expansion of parametric reporting,
  - reasons: necessity to introduce new system functions available in a few languages; expansion of the organization to other countries,
- organizational migration
  - the purpose of this project is to adjust the system to organizational changes,
  - reasons: changes in capital structure such as merger or division,
- physical migration
  - the aim of this kind of project is to adjust the system to localization changes within organization; in some cases, in order to maintain business continuity, it requires establishing a twin system for the period of the project, which may make it extremely costly,
  - reasons: physical organization movement to a new headquarters, moving the server room or changing service provider,
- reconstructive migration
  - the aim of this type of project is to reconstruct the system after a critical situation with regard to source environment (primary IT system working environment); critical situations are, among others: fire, flooding, theft, catastrophe; in some situations, in order to maintain business continuity, it is necessary to have a back-up location for the system; because of the costs, complete functionality is rarely located there,
  - reasons: physical damage of the primary environment, moving the organization to new headquarters after critical event or catastrophe.

4 Resources subject to migration

All types of material and immaterial technical means are subject to migration. The most important ones are presented below.

4.1 Network infrastructure

Network infrastructure encompasses issues related to hardware used for building the computer network as well as type and topology of the network. In case of source system migration both wireless and cable network devices such as: network card, routers, switches, bridges, access points, cables (their type), as well as modems and hardware security solutions have to be taken into account. For the purpose of migration the Table 1 can be used.

4.2 DNS – addressing of computers and devices

An important issue in the migration process is granting addresses to network devices, including end-users' computer systems and servers.

Source system hardware has its own set of addresses for devices, which, depending on the type of migration, may migrate according to the following rules:

- set of addresses and domain names remains unchanged,

Table 1. Migration *(source: self study)*

Device name	No. before	No. after	Remarks
Wired networks			
Ethernet card			
Router			
Switch			
Bridge			
Modem			
Firewall			
Access servers and devices			
Wireless networks			
WLAN card (USB, PCMCIA)			
Access point (AP)			
Wireless router			
Wireless bridge			
Electric network bridge			
Wireless modem (GPRS, EDGE, UMTS)			
Others			
Hardware systems IDS/IPS			
Hardware firewall systems			
Hardware gates			
Wireless Network hardware security			
Radius / Diameter Servers			
IDS/IPS Wireless hardware systems			

- set of addresses and domain names is extended,
- set of addresses and domain names is limited,
- set of addresses and domain names is extended,
- set of addresses and domain names is limited,
- set of addresses and domain names is completely changed.

In case when the ability to ascribe IP addresses and domain names remains within competence of the team responsible for migration, determination of final set of addresses may be formed freely, unless it disturbs organizational, country and international norms.

If, however, changing the IP addresses requires cooperation with third persons, both within the organization and outside of it, it is necessary to include the address changing actions in detail in the schedule of migration, because of the character of DNS [13] system, which is a dispersed base and requires time for refreshing the name servers' content [14].

4.3 E-mail

Among the resources of critical meaning during source system migration, there are issues related to electronic mail, which is a typically virtual concept and encompasses the following problems:

- hardware:
  - determining specifications of outgoing and incoming e-mail servers:
    - determining SMTP applications (Sendmail, Postfix, MS Exchange, Qmail),
    - determining anti-virus applications (clamav, arcavir),
    - determining anti-spam applications (SpamAssassin, Bogofilter),
    - user virtualization (file system or database system),

  - way of communication (introduction of TLS protocols),determining client applications:
    - e-mail clients (Outlook, Outlook Express, Thunderbird),
    - webmail (choice of software),
- procedural:
  - establishing electronic mail domain – this point is strictly connected with point 4.2 concerning addressing issue,
  - establishing account naming,
  - establishing aliases naming (virtual users or procedures of e-mail address construction),
  - procedure for opening and removing accounts,
  - procedure of archiving and security,
  - security procedures with regard to unwanted mail and malicious software.

Determining rules for use of electronic mail should allow minimizing the number of threats, which are related to use of this service.

4.4 Servers

A server is a computer that has been set aside to provide specific services for the benefit of other computers, systems or users. Among the most common types of servers used in organizations are:

- application server[6]:
  - WWW server,
  - DNS server,
  - FTP server,
  - E-mail server (incoming outgoing),
- file server,
- printer server,
- authorization server,
- database server,
- client.

Hardware requirements set for server differ depending on the scope of services they provide and, subsequently, requirements concerning resources. Basic criterion for hardware solutions with regard to servers are: reliability, ability to realize desired redundancy and quick access to particular services. Role of a server may be served by any computer system, however, the above mentioned limitations make it necessary for computer system designers to use components of higher standards and parameters. This refers to elements presented in Table 2.

Table 2. List of elements of a high-end server
(source: self study)

	Server
Number of CPU's	>= 2 (server use)
RAM memory capacity	> 4 GB
Number of PSU's	>= 2
HDD capacity	> 1TB
HDD type	SCSI, SAS
UPS	Required
Air Conditioning	Required
Network card	>=2

Server systems require appropriate operation system, which enables to use multiple CPU's, address high RAM memory capacity and is compatible with other, advanced solutions. They work under the following operation systems:

- Microsoft Windows Server family,
- Linux systems class,
- UNIX systems class.

Choice of operation system should depend on policy concerning software used in the organization or on applications, which will be used on a given hardware.

4.5 Configuration of servers and devices

Installation and configuration of servers, as well as all other devices accessible in an IT system, is an issue which in a direct and key way influences problems connected with security of the whole system. This process should be carried out and, simultaneously, controlled according to procedures provided by hardware and software producers and, with regard to people, by highly experienced staff members.

Installation and configuration of servers may be divided into two main parts: basic installation and installation of applications. Basic installation should consist of the following elements:

- verification of proper hardware functioning (review of BIOS communicates, etc.),
- choice of OS dependant on the server used,
- primary installation of OS and carrying out hardware performance tests in order to eliminate flawed system elements,

[6] Application server [online]. Wikipedia : the free encyclopedia, 2008-01-29 17:45Z [access: 2008-02-27 08:16Z]. Internet address: http://pl.wikipedia.org/w/index.php?title=Serwer_aplikacji&oldid=11141122.

- another, actual installation of the OS in the minimum extent which is necessary for proper functioning of a given server (each unnecessary module needs to be updated, therefore may constitute a security loophole in case it is overlooked during update process),
- configuration of key system modules and limitation of access rights to the necessary minimum,
- determining the server access policy (remote, local, passwords and group of administrators).

Installation of applications may proceed according to different schemes, dependant on the type of application. For example, presented below is the installation process of a WWW server:

- obtaining installation version / binary or source files from a trusted source, preferably with use of checksum verification,
- determining the application location in the file system structure,
- source compilation, installation,
- determining application configuration,
- test-run of application,
- checking application security and limiting access rights to the necessary minimum.

Device configuration mainly consists in:

- determining access to devices,
- drivers installation,
- configuration testing.

Network devices are subject to additional verification of access rights and possibly to software updates, while, because of the role they play, they are often the target of attacks.

4.6 User data

Determining user data is a complex process, because the number of services available in the IT system may change in the process of migration. Depending on the range and number of servers, users of the system may be divided into following groups - see Table 3.

Table 3. Types of users in a system *(source: self study)*

User type	Attributes
System user	name, password, account size, user type, user group, login key, name and surname, location in the organization, range of addresses which can be used in the login system, type of access to resources, determining access to resources
Database user	name, password, account size, range of addresses which can be used in the login system, type of access to resources, determining access to resources
E-mail user	name, password, account size, e-mail address
FTP system user	name, password, account size, type of access to resources, determining access to resources

Table 4. List of elements of steering, measurement and control systems *(source: self study)*

Type	Functions
Driver modules	Devices which directly steer the processes
Measuring devices	Sensors, measuring and record-keeping instruments which computerize information about the process and transfer them to SCADA system
Visualization systems	Audio-visual infrastructure for presentation of ongoing processes, presenting calculations
Wiring	Transmission media which connects the IT system with steering, measuring and control devices

Additionally, it should be pointed out that the user has a configured working environment, sometimes referred to as 'profile', in which some configuration parameters and private keys are stored.

Therefore it is sometimes virtually impossible to perform a complete migration. Security copy of the profile has to be preserved in such a way, that, after some time, it is still possible to reach to some element of the environment which was not needed just after the migration and was simply overlooked.

4.7 Printers

Access to printers which exist in the organizational IT system may be realized through:

- giving access to printer with the use of user computer system,
- giving access to printer with the use of printer server (software or hardware),
- giving access to printer with an in-built printer server module through connection to network infrastructure.

Use of printer server enables detailed determination of printer access rules through determination of user rights, parts of network, access time and number of pages to be printed.

4.8 Steering, measurement and control systems

In case of IT systems connected with steered technological or production processes, system migration becomes more complex due to the need to move, back up temporarily or divide measurement and control signals. Such systems are most often called SCADA.

SCADA (Supervisory Control And Data Acquisition) – system which monitors a technological or production process. Basic functions of SCADA software are:

- gathering up-to-date data (measurements),
- visualization of processes on monitors and synoptic tables,
- observation and change of technological parameters,
- remote control of technological processes,
- generation of information on emergencies and malfunctions,
- supporting operator in extraordinary situations (advice system),
- storing archival data about the monitored process.

Key elements of SCADA are presented in Table 4.

5 Migration project management

Migration process management consists of a range of activities, which are necessary to move from source state to target environment in a pre-defined time period.

Among these activities are:

- activities connected with planning and scheduling processes,
- activities connected with project realization,
- activities connected with project control.

As presented above, migration should be treated as any other project and it is characterized by all the aspects of project management. Apart from realization of the above mentioned activities, migration process also requires limiting risk, ensuring communication between people engaged in project realization and their proper motivation. In the process of project management, we deal with a couple types of participants:

- project manager – key role in the project; his tasks include:
  - coordination of tasks between participants,
  - motivating project participants,
  - elimination of problems and threats,
  - communication with project sponsor and participants
- project sponsor – key role in the project with regard to decisions of highest importance. His tasks include:
  - initiation of project realization,
  - choosing the project manager,
  - taking key decisions,
  - changing project budget and deadline,
- project participant – his tasks include carrying out activities and sets of activities which result from the project plan or schedule.

One of possible methodologies which can be used for migration project management is PRINCE2 [16]. Primarily it was used only to manage IT projects, but now it is a methodology independent from area of use. Characteristic for this methodology is the process approach to project management, in which the following main processes are distinguished [16]:

- directing a project,
- planning,
- starting up a project,
- initiating a project,
- controlling a stage,
- managing product delivery,

- managing stage boundaries,
- closing of a project.

However, because of high expectations concerning the management process itself, this methodology should be used in case of large and very large migration processes. Another methodology, or set of best practices of project management, is PMBOK [17]. It encompasses five fundamental groups of processes [17]:

- initiating processes – elaboration of opening document, elaboration of initial project scope,
- planning processes – project management plan development, project scope management planning, project scope planning, work packets establishment, activity definition, activity sequencing, activity resource estimating, activity duration estimating, schedule development, cost estimation, cost budgeting, quality planning, human resources planning, communication planning, risk management planning, risk identification, qualitative risk analysis, quantitative risk analysis, risk reaction planning, purchases planning, contracting planning,
- executing processes – directing and managing project execution, quality assurance, acquiring project team members, project team development, information distribution, gathering offers from sellers, selecting sellers,
- controlling processes – project work monitoring and controlling, integrated change management, scope verification, scope control, schedule control, cost control, quality control, team management, work development reporting, stakeholders management, risk monitoring and control, contract administration,
- closing processes – project closure, contract closure.

5.1 Organizational activity

Efficient leading of migration project requires the following organizational activities.

- appointing appropriate representatives and teams,
- determining budget for new infrastructure and migration process,
- accepting activity schedule.

5.2 IT agent

Tasks:

- elaboration and coordination of network and systems configuration changes, including development,
- coordination of software and hardware purchases,
- contact with contracting parties: subcontractors and implementation companies,
- software legality control.

5.3 Project and implementation team

Tasks:

- establishing detailed projects within each phase,
- carrying out projects,
- commissioning chosen tasks connected with IT system construction to other units,
- moving proposals for appropriate organizational activity.

5.4 Migration projects execution models

Similarly to any other IT undertaking, we may choose either “light” or “heavy” project management methodology. The more complex the migration project is, the stronger the project management mechanisms, documentation and control, should be developed.

6 Migration scenarios

In the strategic phase, which precedes the decision about project execution, choice of a solution should be preceded by analysis of every possible migration scenario. The best solution may be chosen on the basis of points granted in a pre-defined system of criteria and weights.

6.1 Exemplary criteria and scenario network

Depending on the degree of complexity of a migration project, scope of changes may be divided into activity areas or stages, and a couple of scenarios may be derived for each of them. Choice of scenario for each stage will provide us with the realized path within the scenario network. Appropriate scenario network will enable change of path in case of occurrence of new, significant situations such as change of budget, shortage of staff or change of legal regulation, during the project. It has to be pointed out that, as some stage scenarios may exclude one another, a well-prepared scenario network may help to avoid serious mistakes.

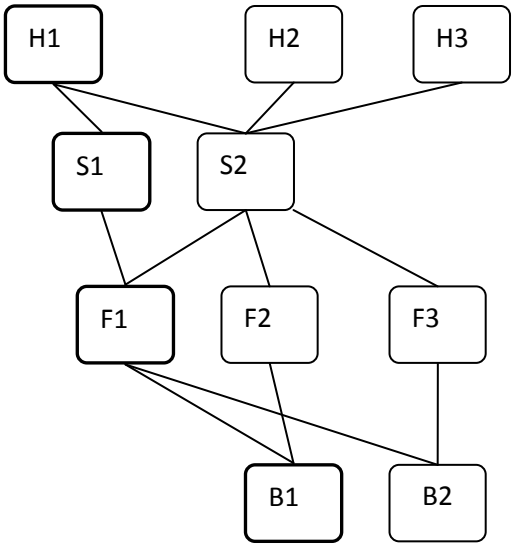

Figure 1. Scenarios Network *(source: self study)*

Network of scenarios, with an indicated chosen path of activity as well as exemplary scenarios, is presented in In Figure 1 it can be seen, that the migration scenario: H1S1F1B1 was chosen. In case of problems with H1 scenario, i.e. delayed procedures concerning hardware or lack of resources for this hardware, a decision about change and choice of another migration path may be taken immediately and it is limited to the H2S2F1B1 scenario or H3S2F1B1 scenario. Having prepared before the analysis of all variants, we decide for H2, which determines the whole path: H2S2F1B1.

6.2 H Scenarios

Scenarios related to choice of hardware:

- H1 Scenario - purchase of new hardware,
- H2 Scenario - installation on existing hardware,
- H3 Scenario - hardware outsourcing.

6.3 S Scenarios

Scenarios related to choice of operation system or database.

- S1 Scenario - S_A operation system, B_A database,
- S2 Scenario - S_B operation system, B_B database.

6.4 F scenarios

Scenarios related to functionality:

- F1 Scenario - full functionality from the moment system is started,
- F2 Scenario - functionality launched in stages,
- F3 Scenario - functionality launched in stages.

6.5 B scenarios

Scenarios related to security:

- B1 Scenario - security in the first place,
- B2 Scenario - resignation from chosen security functions in order to speed up activities.

7 Security design

Each IT system is equipped with an appropriate set of tools which increase its security. Below, the ways of security measures design during system exploitation were presented. On the basis of such schemes, the security measures for the period of migration should be prepared.

Security measures may exist in two forms. In the proactive model, they protect resources before an incident occurs. In the reactive model, they are introduced after the incident is detected. Both models ought to be used, which, in an obvious manner, will form up a security-system lifecycle. Classically, in such system, after implementation there comes exploitation process, which includes periodical modernization sometimes stimulated by incidents. An alteration of reactive model is the system of automatic reaction to an occurrence within the preventive model. In both cases security measures have to be coherent and complete. Coherence means that the security measures will work in different operation systems, locations and cooperating institutions. Completeness, with regard to the idea that the chain is as strong as its weakest link, guarantees that each system within the company has the same level of protection.

Hereafter chosen methods of determining security measures for IT systems will be discussed shortly.

7.1 Security system lifecycle

Process of establishing security measures does not differ from generally known IT systems construction schemes. Such stages as analysis, design, implementation and current performance analysis may be distinguished during exploitation of security measures (Figure 2). Details of actions, which will be taken in the higher stages, introduces wide variety of security measures design methods.

Knowledge from analysis or set of conditions resulting from security policy provides us with the boundaries, within which we should generate security elements.

In case of migration, life cycle looks the same. After the migration is finished, security measures undertaken for the period of migration will be removed.

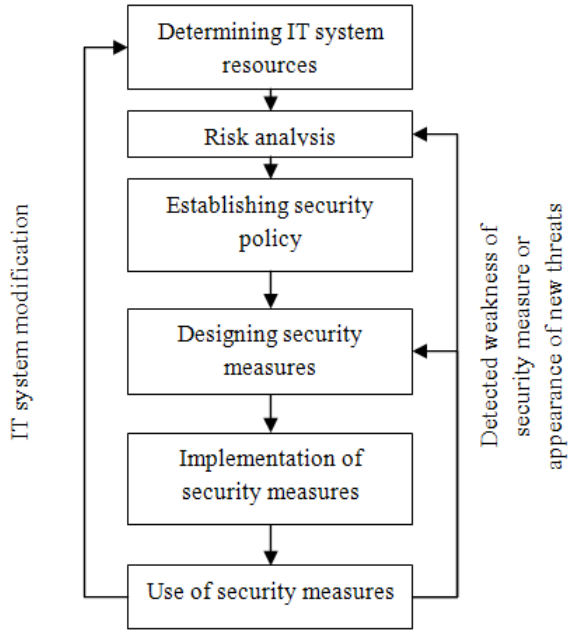

Figure 2. Lifecycle of security measures
(source: self study)

The above scheme requires little comments. The process of determining IT system resources consists of: stocktaking, classification and valuation. Under risk analysis we understand the identification and validation of threats, evaluation of existing security measures, evaluation of losses, determining the acceptable level of risk.

7.2 Expert method

When using this method we consciously resign from extensive analytical processes which precede the choice of security measures.

In many cases a good way to deal with the issue of improving security in a company is to hire a well-trained IT security specialist. After performing a not too detailed analysis of IT resources, without risk analysis and without distinguishing security requirements, security elements may be designed. This method proves effective in case of relatively uncomplicated systems. Especially in this method it must be stressed, that the system security level is determined by its weakest element.

Security measures in different layers should overlap in such a way, that shortages of one layer will be compensated by another one. In most cases, however, project of security measures should follow a proven methodology.

Expert method does not allow us to evaluate losses, that may be incurred in case of some threat coming true, which is necessary even when we want to insure our resources.

7.3 Choice of security measures based on risk analysis

This method of choosing security measures requires careful analysis of risk related to company resources. An anticipated result of this process, apart from choosing technical security measures themselves, might be all kinds of security policy elements. They might be treated as a sort of security measures as well. For example, security officer, who is an element of security policy, can be treated as a security measure for the purpose of cost analysis.

Risk analysis is one of the elements of risk management process. Identified risk becomes accepted and has to be controlled. Below (see Figure 3), we present a scheme of relationships between security elements, which presents the access path to resources from the environment. Access is always burdened with risk, even if, in case of introduction of security measures, only residual risk is left. It must also be taken into account.

Polish Norm PN-I-13335-1:1999 includes the following definitions:

- risk - probability, that a given risk will address resource or resource group vulnerability, resulting in losses or damaging the resources,
- residual risk - risk which remains after introduction of security measures,
- risk analysis - risk identification, determination of its size and identification of areas which require introduction of security measures,

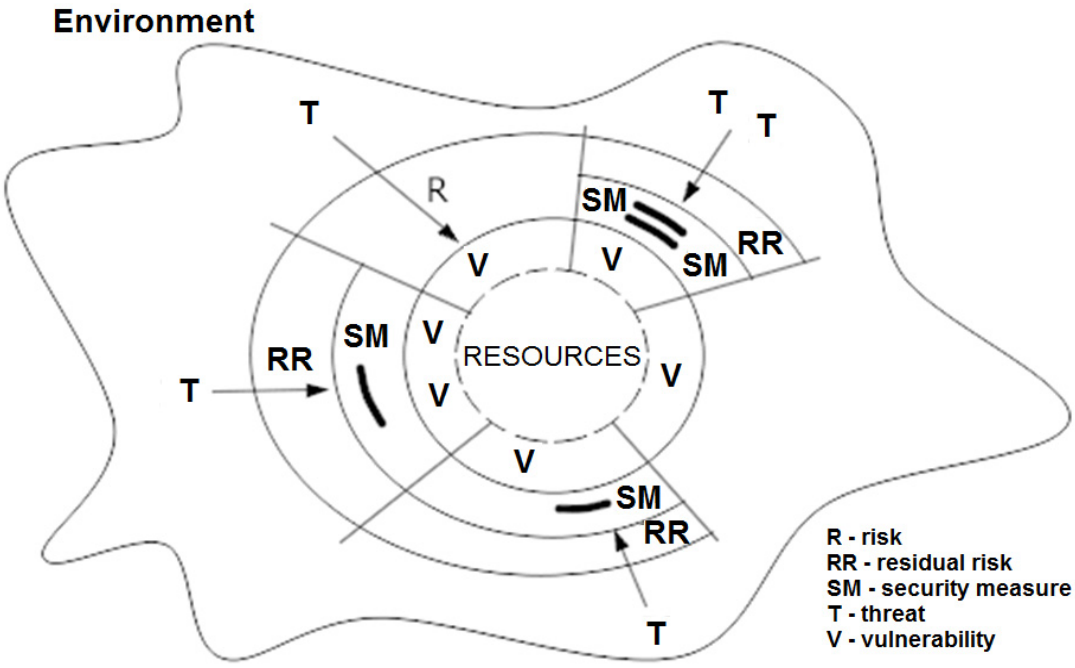

Figure 3. Relationships between security elements (PN-I-13335-1:1999)

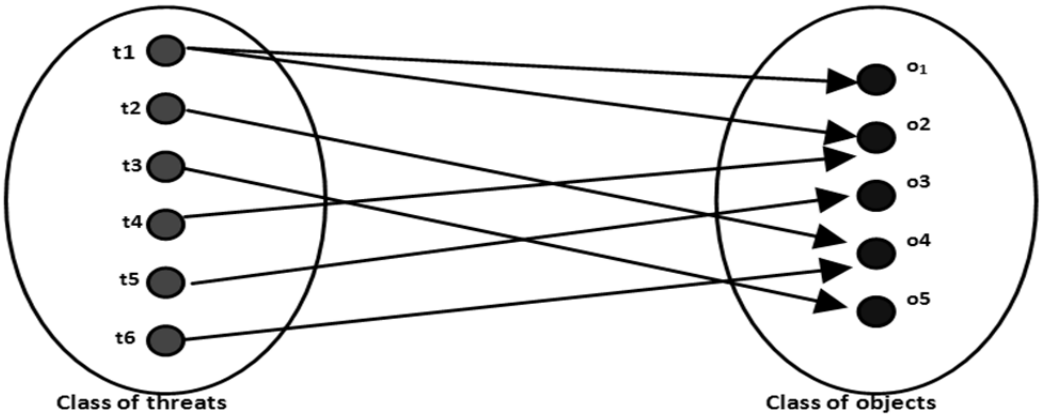

Figure 4. Identification of all possible entrances – threats
(source: self study)

- risk management - complete process of identification, controlling and elimination or minimization of uncertain events' occurrence probability, which may have influence on IT system resources,
- threat - potential cause of undesirable incident, which may result in harm to system or institution,
- vulnerability - resource or resource group weakness, which may be used by threat,
- security measure - risk-reducing practice, procedure or mechanism.

The set of threats is only partially known and undergoes constant changes in time. Process of analysis provides us with detailed information on resources access paths, as presented in Figure 4.

The best measurement of risk is cost incurred by the firm in case of an incident. Unfortunately, there are a lot of situations, in which such a cost is very hard to measure, as in case of company image and loss of potential orders. Nevertheless, each of the identified paths is burdened with risk of potential loss connected with improper access to resource.

Because we are not able to precisely determine the risk, one or a couple of methods of calculating risk should be used simultaneously, i.e. best case scenario, worst case scenario, most probable scenario.

Table 5. Points referring to risk *(source: self study)*

Risk level	No. of points	Description
High critical	5	Organization (system) loses ability to function. Serious economic results.
High	4	Organization (system) functions, but in each moment may lose this ability
Medium	3	Visible disruptions in company functioning.
Low	2	Minor obstruction of functioning, which rarely disrupt normal functioning
Low acceptable	1	Acceptable obstruction
None	0	System element which is irrelevant for the functioning of the whole system

In many cases, it will be enough just to calculate risk by attributing points, which refer to the greatness of this risk (Table 5). The table is based on a three-level security mechanisms evaluation system, introduced by a certifying unit UOP (from European ITSEC). However, greater gradation of threats was introduced.

Having determined the level of losses, we can impose security measures on chosen system vulnerabilities, with regard to appropriate paths of access to resources (Figure 5). In this way, we set a new level of resources security. As we have calculated risk for each vulnerability, we can, in every moment, answer the question: What risk is left with regard to resources? Therefore, we are managing risk to resources. Lack of activity formalization in this method requires using trial-and-error method tests of the fact if level of risk is acceptable. It would be harder to reverse the problem, define the acceptable risk and try to find a set of security measures, especially in highly developed systems.

This method is satisfactory when we decide to secure all existing resource vulnerabilities. Sometimes it is impossible, and the level of security may vary as well. When looking for some more precisely determined level of risk, it is necessary to apply optimal choice of security measures method, which exceeds the scope of this paper.

8 Security in migration process

During the migration process, especially essential becomes the care for IT resources security. IT resources, which in normal work conditions are covered by security procedures, may unwillingly become endangered by threats in different system environment.

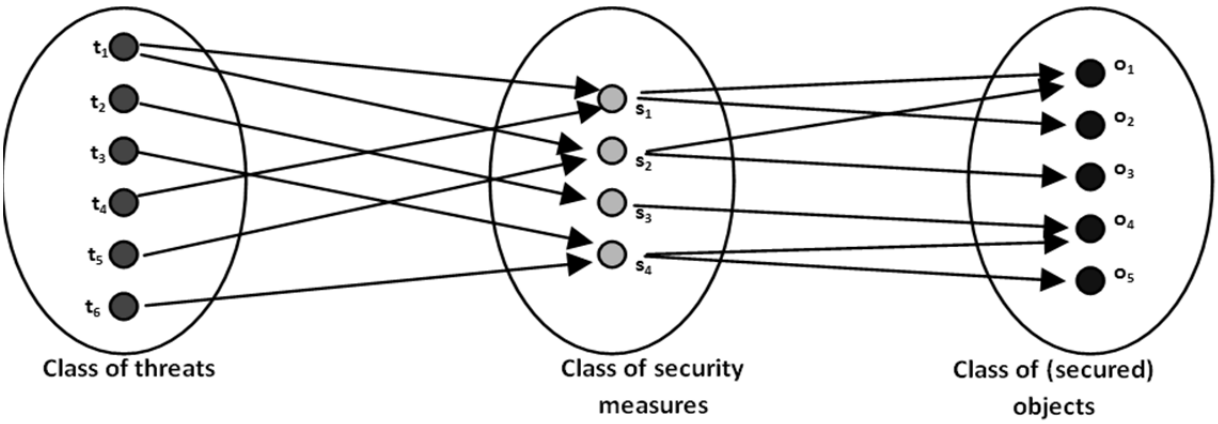

Figure 5 Complete security system
(source: self study)

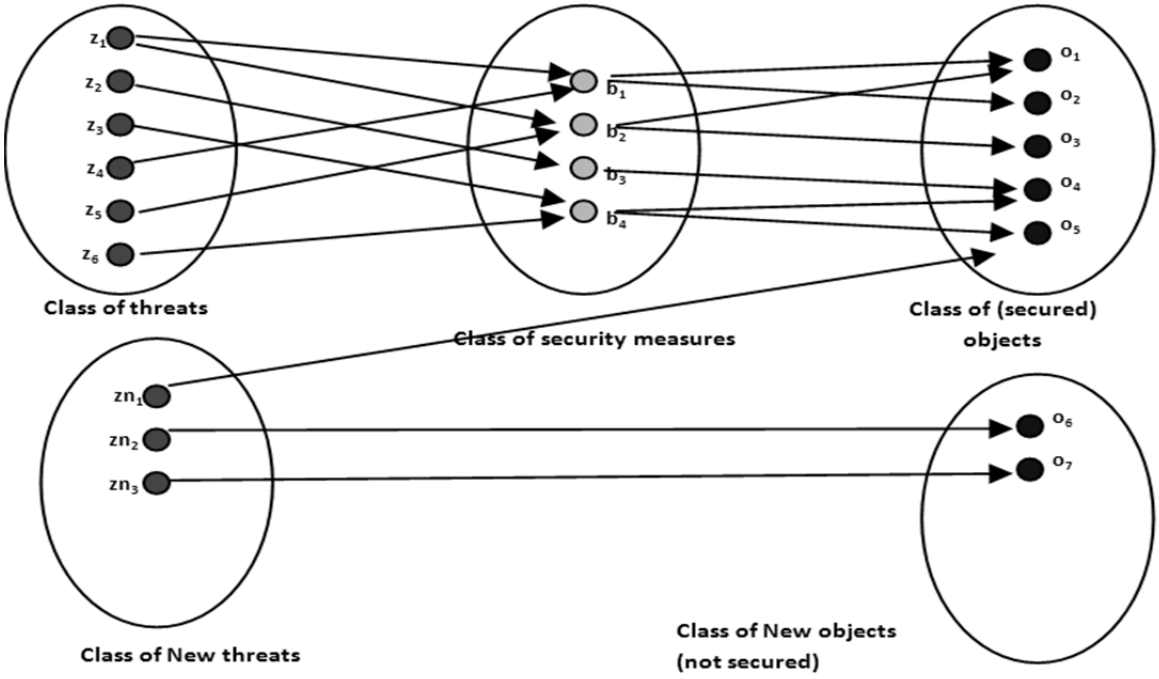

Figure 6. System during migration process
(source: self study)

8.1 Threats

During migration process, new threats appear which influence old resources (O1-O5 objects) as well as new resources (O6-O7 objects). In both cases, the interactions are not secured (see Figure 6).

Appropriate security action must introduce security measures for the purpose of resource protection. Below, exemplary threats which appear during migration process are described.

8.2 Additional accounts with higher system rights

Migration process is full of different types of tests and installations. For most actions, additional IT system accounts, often with too high rights, are added. Appropriate procedures and system rights structure may prevent interference of unauthorized persons with key system elements. Deleting such accounts must be attended to immediately after the process is finished.

8.3 Moving data

Process of moving data from source environment to target environment may be carried out according to the following schemes:

- directly between systems – original data may be damaged; it is necessary to prepare and test security copy in advance,
- moving of prepared data copy through chosen e-communication channels: http, ftp, e-mail – it is necessary to secure channel or data, i.e. by encrypting them,
- physical movement of data copy on a given storage device – it is necessary to secure data. i.e. by encrypting it and by physical protection during transport.

The above mentioned list implies the fact that we will have to cope with many versions of data copies, placed on different storage devices. Wrong choice of copy version, losing a copy or interception of a copy, i.e. on an old hard drive taken from a server which was put aside long ago, may all have serious legal and economic consequences.

8.4 Softening of security measures

Tight schedules of IT projects seem to be a good enough reason for softening the restrictions in the processes of granting rights or opening accounts. Certain administrative activities which improve system security are postponed for later periods and are often never executed.

8.5 Security systems shutdown

For the comfort of and in order to speed up some administrative and servicing activities, there will always exist the temptation to temporarily switch off chosen security systems. During migration process there are a lot of such activities, which may lead to prolonged periods of decreased threat-resistance. It is also more likely to leave systems without unsecured for a couple of days.

8.6 Remote access

Because of their systems' security, many companies do not allow direct connection with the internet. System migration is often handed over to external companies, which, for their own comfort, insist on the possibility of remote access.

If a company does not have proper infrastructure and experience to grant such an access, it can easily expose itself to trouble connected with data interception or network intruders. At this point, it is extremely important to introduce proper organizational and legal protection in the contract with the cooperating entity.

8.7 Hardware replacement

When one of elements of migration is hardware replacement, a problem appears of managing the used-up hardware. Scrapping, selling off to employees or utilizing do not lift the obligation to properly remove the data from the storage devices. Well known media cases of obtaining such data by journalists are the least severe punishment for this type of mistake.

8.8 New system break-in

As mentioned before, a newly introduced system is more vulnerable to all undesirable activities of third parties. Most common effects of breaking in are:

- introduction of changes to the attacked system (i.e. modification of password list, changing system software files),
- installation of modules such as Trojan horse or so called Sniffler,
- intrusion in private matters, i.e. reading someone else's e-mail,
- causing moral losses (i.e.: changing the content of web pages, distributing pornography).

8.9 Security

Gathered below are the most important protective factors, which improve security during migration:

- adequate procedures of system access, data access, moving and copying data; procedures which cover the entities which cooperate in migration process; appropriate legal protection in contracts with cooperating entities,
- physical protection: special control over all devices belonging to the key IT infrastructure elements of source and target environments (servers, switches, routers); installation of infrastructure in dedicated, air-conditioned, secure rooms,
- use of uninterruptable power supply: securing key IT infrastructure elements from instability or temporary lack of power supply; extremely important during installation of systems and moving data,
- use of uninterruptable power supply for air conditioning and back-up air conditioning; extremely important in server rooms with high power density,
- excluding target environment network from production infrastructure allows basic protection against unauthorized access,
- policy for creation of safety copies,
- policy for protection of security copies; storing, transporting and disposal,
- software updates: before launching system for production work it is necessary to take care of all software updates.

9 Other issues

Among other issues closely related to migration process technology and organization, version management for infrastructure elements, legal regulations and choice of appropriate organizational activities have to be pointed out.

9.1 Legal status

IT security, as mentioned before, is only one piece of information security of an organization. Organization operates in its specific legal environment. Legal regulations are also used in extraordinary company situations and everything has to be done to ensure that all actions are in line with these regulations.

9.2 Legal acts and regulations

Knowledge and use of detailed regulations for particular industries and chosen areas of company activity are obligatory. Nevertheless, this regulation do not impose specific solutions. Most of the time, they have organizational character.

For our considerations, from the legal acts mentioned below the ones of organizational character, which may be used in various ways, should be chosen. With regard to these acts, research of cost-optimal or minimum-loss solutions should be carried out:

- Banking Law,
- Accounting Standards,
- Personal Data Protection Act, 29 August 1997, Official Law Journal of 29 October 1997,
- Prime Minister's decree regarding fundamental security requirements of IT systems and networks of 25 February 1999, Official Law Journal No. 18, pos. 162,
- Confidential Information Protection Act,
- Electronic Signature Act,
- Copyrights Act,
- Act on protection of chosen electronic services based on conditional access.

9.3 Standards and normative acts

IT security is subject to standardization at different levels: international, regional, state and in different sectors of economy: military, banking, industrial, etc. Interconnections between standards and new standards raising from the others are natural processes. In case it is not regulated by separate law, it remains a dilemma, which standard should be considered most appropriate for particular solutions.

Examples shown below are an international standard and a methodology for IT system security management. Both examples have organizational character and, similarly as before, after elaboration of their formalized version may be used as elements of established methods of searching for optimal solutions:

- ISO/IEC 17799:2000 Standard,
- TISM methodology (Total Information Security Management).

9.4 Versioning

In the course of creation of IT solutions, starting from simple, independent applications, ending with complex, multi-module systems, the problem of proper version designation arises. In reality, every team has its own, elaborated system of application, module and documentation versioning. All the methods are based on similar rules. One of them is presented below[7]:

- version scheme:
  <version number>–<version category>, where:
  - version number – series of digits and dots which designates version,
  - version category – additional attribute assigned to versions, which serve a special purpose,
- version number has its specific "sub-scheme", which looks as follows:
  <major>.<minor>.<path/build>,
  where major, minor and path/build are digits; the last element (path/build) may be omitted, if it equals 0 (zero):
  - major – this number characterizes a version, which, in comparison to the previous one, consists significant changes, which are not just "cosmetic" but are connected with important aspects of application functioning; it might be i.e. new way of client interface, new type of data exchange or whole new way of system functioning,
  - minor – this number designates introduction of new elements to application, which do not cause considerable changes in the whole application structure; it may be i.e. addition of new buttons or other elements, which, after contacting the client, led to changes aiming at improving application functionality,
  - patch/build – this number designates introduction of patch which fixes error/errors which were observed or program compilation number (incremented by compiler),
- version category – in order to ascribe an additional attribute to versions, specific categories are used:
  - develop (abbr. dev or d) – category for applications which are in development stage; accessible for a certain group of people (developers or trusted team members),

[7] http://phppl.ezpublish.no/wortal/artykuly/pomysly_porady_sugestie_dobre_nawyki/wersjonowanie_aplikacji; Michał Golebiowski.

  - alpha (abbr. a) – category for applications which went through a vote – was accepted by group of developers to undergo further tests performed by them,
- beta (abbr. b) – category meant for wider group of testers – project members who mainly deal with application testing,
- release candidate / release (abbr. rc or r) – category for applications meant for all the interested people; consists of smallest number of errors in comparison to the above mentioned categories; it is a partly finished project, with most possibilities of the final product; most of the times, such application is aimed at improving those elements, which are considered badly solved by the end user (program navigation, colors, etc.) and those errors, which were not observed erlier,
- final (abbr. f) – final version which goes to the client; this category is usually not added to the version; one can add additional number to category, such as rc 1, rc 2, which will denote another "substage" in application versioning; the higher the number, the "faster" it comes to the next category (there is no upper limit in ascribing additional numbers, however they should not exceed 5).

Examples:

- 1.0 – first final version,
- 0.1-dev – application in development stage, which does not contain all the elements of "full" version,
- 2.2.43 – final application which contains certain corrections with regard to version 2.0 and patched loopholes,
- 1.0-rc – first version of application, which is intended for testing by people from outside.

10 Summary

Modern organization which operates within market economy uses a wide spectrum of information technologies both to run fundamental business activities and to support all kinds of internal processes. IT infrastructure is threatened by constant changes.

This article shows in a methodic way the approach which leads to IT system migration into new information environment. Weight of this issue cannot be overestimated in the situation, when after a few years or because of an organizational change, the company is forced to introduce fundamental changes to its IT system. In order to execute this activity effectively, it is important always to adopt the informatization strategy – unfortunately, it is not a common phenomenon and hardly any organization systematically updates its business strategy and related informatization strategy.

IT system migration is always a serious threat to business continuity, from the point of view of business and information security. As mentioned in the beginning, the awareness of the company security issue is rising. Because the scope of services offered with the use of IT solutions, for supporting and running business, becomes bigger and bigger, IT security plays the key role with regard to business security. Consequently, market demand for introduction of the security policy, both for the period of changes and standard exploitation, increases.

Unfortunately, there is a certain shortage of methods which could support optimal choice of security measures for company resources. Finding fast and efficient methods of minimizing costs and risk can considerably accelerate improvement of security in many companies. At the same time, it can lead to faster company growth.

11 References

[1] *Polish norm PN-I-13335-1:1999*.

[2] Denning D.E. - *Information Warfare and Security*. Addison-Wesley, Massachusetts 1998.

[3] Pipkin D.L. - *Information Security*. WN PWN, Warszawa 2002.

[4] Krupa T. - *Projektowanie strategii informatyzacji* [in] Przedsiębiorstwo w procesie globalizacji (ed. T. Krupa). WNT, Warszawa 2001.

[5] Krupa T. - *Zarządzanie informacją w zakładzie ubezpieczeń* [in] Podstawy ubezpieczeń. t. III. Przedsiębiorstwo (ed. J. Monkiewicz). Wyd Poltext, Warszawa 2003.

[6] Pięta S. - *Metody doboru zabezpieczeń w systemach informatycznych* [in] Komputerowo zintegrowane zarządzanie (ed. R. Knosala). WNT, Warszawa 2003.

[7] Pięta S. - *Metody doboru optymalnych zabezpieczeń informatycznych na potrzeby przedsiębiorstw* [in] Informatyka w przedsiębiorstwie (ed. T. Krupa). Oficyna Wydawnicza PW, Warszawa 2004.

[8] Stokłosa J., Bilski T., Pankowski T. - *Bezpieczeństwo danych w systemach informatycznych*. WN PWN, Warszawa 2001.

[9] Kifner T. - *Polityka Bezpieczeństwa i Ochrony Informacji*. Helion, Gliwice 1999.

[10] Schneier B. - *Applied Cryptography*. Second Edition, John Wiley & Sons, New York 1996.

[11] Molski M., Opala S. - *Elementarz bezpieczeństwa systemów informatycznych*. Mikom, Warszawa 2002.

[12] DiS - *Migracje ERP 2005. MERP 2005*. Raport DiS. Warszawa 2005.

[13] IANA - *Internet Assigned Numbers Authority*. http://www.iana.org/, June 2010.

[14] ICANN - *Internet Corporation for Assigned Names and Numbers*. http://www.icann.org/, June 2010.

[15] IFPUG - *International Function Point Users Group*. http://www.ifpug.org/, June 2010.

[16] OGC - *PRINCE2*. http://www.ogc.gov.uk/ methods_prince_2.asp, June 2010.

[17] Project Management Institute - *A Guide to the Project Management Body of Knowledge*. Third Edition, Paperback PMI, PMBOK Books, Newton Squeare 2009.

[18] Morimoto R., Noel M., Droubi O., Gardinier K., Neal N. - *Windows 2003 Server. Księga eksperta*. Helion, Gliwice 2004.