HADMÉRNÖK

XIII. Évfolyam 2. szám – 2018. június

SECURE MAINTENANCE OF ELECTRONIC INFORMATION SYSTEMS IN PUBLIC SERVICE

KÖZSZOLGÁLATI SZERVEZETEK ELEKTRONIKUS INFORMÁCIÓS RENDSZEREINEK BIZTONSÁGOS ÜZEMELTETÉSE

MEGYERI Lajos

(ORCID: 0000-0002-3743-1520)

megyeri.lajos@uni-nke.hu

Absztrakt

The following paper summarises the permanent principles of electronic data processing in public service, according to which all the basic law and local regulations have been set. It presents the recent system of rules defining the area, which are reset periodically by the creators according to the changes in data processing systems and to be able to meet the appearing new threats, however they remain unchanged in their spirit. The publication has a view also on the regulation and possibilities of providing risk analysis during the planning, shaping and maintaining of information systems.

Keywords: *security, regulation, maintenance, risk, management, vulnerability, threat*

Abstract

Az alábbi publikáció összefoglalja az elektronikus adatfeldolgozás állandó elveit a közszolgálatban, amelyek alapján a specifikus szabályrendszerek kialakításra kerültek. Bemutatja a területet jelenleg meghatározó szabályrendszereket, amelyeket a jogszabályalkotók rendszeresen módosítanak az adatfeldolgozó rendszerek változásai szerint. Így a szabályozás képes megfelelni a megjelenő új fenyegetéseknek, azonban szellemében változatlan marad. A kiadvány az információs rendszerek tervezésénél, kialakításánál és fenntartásánál is foglalkozik a szabályozással és a kockázatelemzés elkészítésének lehetőségeivel.

Kulcsszavak: *biztonság, szabályozás, fenntartás*, kockázat, menedzsment, sebezhetőség, fenyegetés

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.01.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.06.10.

INTRODUTION

Development of electronic assets has been speeding up by leaps in the recent decades. We are surrounded by devices consuming electric energy, and we are more than ever depending on them. It is enough to imagine a simple shortfall in electricity, life almost stops, in lack of electricity the operation of basic infrastructure can be jammed, even work can stop. Electronic tools occupied space in the most different areas of life. With their utilisation, flow of information has speed up in an unbelievable pace, new horizons emerged in the field of data processing as well. Creation and then the spread as mass article of the computer has sent new areas of science on their way. The category of informatics came to life, the terms of which aren't forming a common form in different languages, which, in case of multinational work – for example EU, NATO information systems – is an extra task to be dealt with.

Flow of information getting faster, the possibility to contain and process an amount of data yet unimaginable has led to the question of security as well. During history there has ever been such information that had to be protected from people with harming intentions against the legal possessor of the information. With the spread of information tools, the growing quantity of data and the appearing of services not existing earlier, also the requirement of making these activities secure emerged in an instant. At the beginning, local workplaces and systems had been protected by the maintainers via rules according their own aspects. Connecting the systems and the network becoming international made the standardisation of the regulation necessary, which is a never ending, constant activity. Beyond clarifying the basic terms, I'd wish to have a view on the international regulatory system and its Hungarian aspects as well in this paper.

BASICS OF INFORMATION SECURITY

Fields

Information security comprises of the sub-areas as follows:

- personal security,
- document security,
- administrative security,
- electronic information security.

These fields can basically be separated from each-other, however sometimes they can overlap. For example human, personal factor appears also on the field of electronic information security, like the dimension of creating and maintaining software protection.
It's basic that with the creation of information protection the protection of data has to be secured as key element. This can be realized through the physical protection of devices and places, by restricting the access of persons to data, and with utilization of administrative regulations and softwares. Thus it is important to define the term data.

According to Law L of 2013, data is defined as: *„the carrier of information, formalised depicting of facts, notions or orders, which is suitable to be transmitted, visualised or processed to people or automatic devices*"[1]

Basic terms

Security:

The state of the system in which a closed, full-spectrum, and permanent protection is realised which is in balance with the risks. Thus security is a status.

- *closed protection:* protection counting with all the possible threats.

- *full-spectrum protection:* protection covering all the elements of the information system.
- *permanent protection:* protection being realised without break also among circumstances changing through time.
- *protection in balance with the risks:* the protection of the electronic information system, during which the price of the protection is in balance with the expected costs of damage caused by the threats.

Security as an ideal state doesn't exist. We always have to strive for a protection in balance with the risks, on one hand in order to utilise resources (e.g. money) effectively, otherwise because the increase of security goes together with the decrease of the system's effectiveness. The applications monitoring and filtering malwares, the devices and methods making access to the workplaces physically more difficult, and obligatory administrative steps slow down and block the work with the system.

Thus while planning the information system, avoiding of down planning and over planning has to be of central importance within the processing of security measurements.

Protection:

Activity, also row of activities, sum of regulations, which directs towards the realisation, keeping up or building up of the state called security.

Goals of protection:

- *prevention* (avoiding the realisation of the effect of threat)
- *early warning* (forecasting an expected occurrence of any threat in time to be able to take appropriate protective steps)
- *sensing* (realising the occurrence of the security event)
- *reaction* (measurement taken to ban or slow down the escalation of occurred security event, and decrease further damages)
- *event maintenance* (documentation of the occurred security event within the electronic information system, elimination of the consequences, determination of the reasons and responsible people for the event, planned activity in interest of avoiding the re-occurrence of similar security events in the future)

Basic principles

Principle of necessity and proportionality: the right of access to the publicity of data of common interest can only be restricted in case of circumstances defined by the regarding (CLV of 2009) law, with the level of classification required by the protection and to an inevitably necessary time only.

Principle of necessary knowledge: classified data can only be known by those, who inevitably need it to meet their state or public tasks.[1]

According to Law CLV of 2009.[2] the followings have to be secured during the handling of classified data:

Intimacy: *„the feature of the electronic information system, that the contained data and information within can be learned, utilised and being ordered to be utilised only by those being authorised and only by the extent of their authorisation."*

In open-access data processing systems, central data storage is common, where all users of the system are able to reach the database (e.g. the library of files arriving to the unit). This

[1] This is called the principle of „need to know" in international regard.

enables quick change of data, and effective work. As a drawback, each user is able to learn also information not necessary to their own work. Since these data are not classified, this doesn't mean aggression on secrecy. The personnel refreshing the database has to be highly aware that data affecting personal rights (e.g. regarding health or criminal record) cannot be saved to a storage reachable to anyone. A good solution can be the so called Information Management System (IMS) introduced with the Hungarian Defence Forces, which processes open access data, but the circle of people being able to reach it can be defined, and the fact of access, the measurements taken and the files created in connection with the case are documented in a retrievable form by the IMS system.

Integrity: *„the feature of the data, referring to the content and features of the data being identical to the expected, this meaning also security in that the data is stemming from the expected source (credibility) and in that the origin is verifiable and solid (undeniability), beyond that the feature of the electronic information system, that each element of the system can be used according to its call"*

It means that the data handled via the system is equal in all its features with that prepared by the user. This can be secured with the restriction of access to the data preserving hardware elements, by utilizing CRC[2] failure detecting method, or for example with the using of Hash[3] function also used at the electronic signature.

Disposability: *„it has to be secured, that the required data can be reached by the authorised persons in the right time, in proper form and with appropriate content*"

This means, that the user is to be able to reach the data contained in the system at any time in the extent required to do their work. With open access information systems this is quite easy to realise, the refreshing, maintenance, replacement of broken system elements, hardware, software can be done rather easily complying with basic logistical regulation. Maintenance or replacing of elements in an information system, handling classified data is regulated by strict rules, any deviation from which can mean a security event.[4]

DATA HANDLING

About data in general

In the field of electronic information protection, data is regarded mostly as document file on the level of everyday use. Beyond that also constantly operating networks exist, which provide a service securing ongoing work – e.g. transmitting of radar data.

We regard defining the term of data handling also important, because each activity connected with data can be regulated based on this.

According to the National Magistrate for Data protection and Information Freedom, data handling is defined as:

"with disregard to the utilized process, any operation done to the data, e.g. collecting, recording, securing, organising, containing, changing, using, requesting, transmitting, announcing, coordinating, banning, clearing and discharging of data, beyond that the prevention of further utilisation, taking of picture or voice material, and the recording of

[2]CRC: Cyclic Redundancy Code
[3]Hash function – one way algorithm to secretase
[4]*security event:* unwanted or unexpected casual event, or chain of events, which creates an inclement chnge or a situation not known before in the information system, and as an effect of which the confidentiality, intactness, credibility, functionality or disposability of the information carried by the electronic information system is getting lost or damaged. Law L of 2003. 1. § (1) 9.

physical characteristics applicable to identify a person (finger or hand print, DNA sample, iris picture etc.)"[i]

A similar definition can be found in the 94/2009 order of the MoD, which gives obligatory guidelines to the organisations, directly subordinated to the Ministry.
Basic principles are equal, but the regulation regarding execution is differing between the civilian and military fields of utilisation. In civilian regard the main bulk of tasks comprises of processing personal data, data of common interest and those being open access out of common interest. These can be called open access data in general. In the military sphere however, most of the data belongs to the open, restricted access category.

The process of open access data is regulated by the Law CXII. of 2011. It defines the types of data, and the order of data processing.

On information security measures, regarding the maintaining of electronic information systems 41/2015. (VII.15.) order of Ministry of Interior is giving guideline. According to it, electronic information systems have to be categorised into security classes. The classification is verified by the leader of the organisation based on the data processed and on risk analysis. The function of each system element and the type of processed data is also of key importance.

In case of protecting data, different security elements are regarded to be primary, based on the processed data and the service provided by the system: in case of systems processing data property of the nation, requirement of intactness is focused on; regarding vital information systems, disposability is required primary; in connection to special personal data, maintaining confidentiality is defined as a basic need.

Data processing at armed and law enforcement forces:

On all fields of defence sphere, confidentiality is of high importance. Disposability is also important, but gets only second during the maintenance of information systems. Putting it easy: a data may rather parish then to get into wrong hands.

Regarding their confidentiality, data can be:

- open access
- classified

Although in military regard the category of „open, restricted access" data is present, the main bulk of tasks for personnel working with information security comprises of processing „classified" data.

On data processing at HDF 94/2009 MoD order[3] is clarifying the regulation of the law. The order tells that also no classified data has to be put into security classes according to the following:

"a) no classified data has to be categorised as basic security class;

b) classified data of large quantity, special data, business data, address data, and maintenance data have to be categorised into class of increased security to secure higher level of utilising security requirement."

Increased protection of classified data is basic obligation also ordered by law. Beyond this, the regulation also defined the nonclassified data to be put into two classes, in which also a certain amount of open access data is wished to be given increased level of protection.

3/2012. (I.13.) order of MoD[4] has clarified the security measurements, and ordered that „the security requirements have to be realized through certain protective regulations and measurements, which have to be defined, verified and utilised in the form of Electronic Information security Regulation (EIsR)."

The open information system of HDF belongs at least into 4th security class according to the regulation. Thus the rule puts requirements also against the information systems processing nonclassified data. For example also STN system of HDF is working according to

this. EIsR contains the local regulation for confidentiality, intactness and disposability of open access data in detail. The regulation has to be known by all the users of the system.

15/2017 (IV.28.) order of MoD is dealing in detail with the official supervision of defence aimed electronic information systems. [5] According to the regulation, the professional personnel of Military National Security Agency (MNSA) are maintaining official's right above these systems. This is an absolutely new and differing order of measurements compared to the former, but it clearly will increase the security of the work of these systems.

Processing classified data

According to Law CLV. of 2009. [2] on the protection of classified data[ ] classified data are:

„*a) national classified data:* data belonging to the circle of common interest protected by classification, bearing classification according to the form requirements regulated by this law and other regulations announced in accordance with it, about which – with disregard to the form of appearance – the classifier determined during the classification process, that the announcement, unauthorised access, modification or utilisation, granting access to unauthorised persons, and also the banning of access to authorised persons can harm or threat (detriment in the following) directly any of the common interest protected by classification, and in regard of its content, it restricts the openness and the possibility to be known within the frame of classification;

b) foreign classified data: every data prepared and provided in accordance of any international contract or agreement announced in law, by all institutes and organs of the European Union, furthermore the states, partaking party or international organisation proceeding in the name of the EU, to which the access is restricted by the institutes and organs of the EU, the state proceeding in the name of the EU, any other state or partaking party, or international organisation."

Law CLV. of 2009. on the protection of classified data describes the circle of classifiers in detail, the classification process, the utilised signature and the general rules on security of classified data.

The novelty of great importance in this law is, that it orders the same protective measurements to be utilised in case of the national classified data, as in that of the foreign ones. Until the announcement of this law, protection of national classified data was put under lower level of physical protection requirements than for example NATO data.

After Hungary joining NATO, the information security requirements have been defined by C-M(2002)49 directive[5]. According to this has the creation of „NATO T Offices" to store and process NATO classified information began, with great financial initiative. Physical and administrative conditions had to be shaped according to NATO guidelines, which is a common requirement towards all the member states. Hungarian state had to create these conditions, which however were only regarding NATO's classified material. National classified data could have been processed under conditions of much lower protection according to the regulation of the time.

Law CLV. of 2009. [2] ended this duplication, and introduced the foreign (e.g. NATO) protective measurements also on the protection of national data. This change caused great problems to the law makers and the executioners as well on the short turn. Building up a protecting system providing high level physical security if of great cost. In the executive orders the final deadline for building the needed physical protection has been delayed for

[5]Security within the North Atlantic Treaty Organisation (NATO). C-M(2002)49. North Atlantic Council, 2002.

years to be able to create the required circumstances from HDF funding. The 161/2010 Governmental order on electronic security and official supervision of classified data has a regulation even more detailed than that of the law.

All the regulations put an emphasis on the necessity of estimation and handling of risk during the process of classified data.

RISK MANAGEMENT

In general:

In our complicated world of today, through the specialisation of scientific fields, serious amount of knowledge has been collected on risk analysis on each field of life.

Avoiding all risk, the state of absolute security can sadly not ever be reached. All creature, device, system and society are vulnerable. Endless time, money and labour cannot be provided to create security. The reasonable utilisation of resources is needed, and that is where exploring and analysing risk can provide help.

Quick development of computer devices has led to the emerging of ever grooving information systems (e.g. Internet). Information networks have emerged and developed at the beginning as independent workstations, then as local networks remote from each-other. Reaching a particular size, in order to reach common goals, and the interest of connect ability, the planners of the information networks had to create common order of measurements. By the growth of the size and complicatedness of the systems, vulnerability of each system-element has also increased. Systems of patterns have come to life, in which differently, but from the very beginning the need of managing risk has been present.

In regard of expected effects, the circle of risks can be divided into two major groups. The first being the group of simple, pure threats, in which cases possible outcome can be: (a) damage, loss occurs, (b) or no change happens. Contrary, we speak of combined, speculative risk, if the risk in question can be followed by three types of outcome: (a) damage, loss occurs, (b) or no change happens, (c) the outcome is profit, gain.[6]

At the exchange market for example, we can speak of taking speculative risk, when the broker decides, what sort of stock to buy, and what to sell. Each stock has a different rate of profit –income, but also the amount of risk taken is differing. The broker can consider how big a risk he wants to take for the expected profit.

We regard the risks of information systems as being those of the pure type, we take risk with no expected income, „only" the risks threatening the constant work of the system have to be dealt with.

On the long term, greater risk, fewer security elements can make realisation of information systems cheaper. Still it is necessary to provide our security system with sufficient protection according to a risk analysis, thus we can create an effective protection against relevant threats, and at the same time we don't bind resources to meet irrelevant threats. Sadly it's not easy to bring the owner, or decision maker to utilise financial resources for protection, since the avoided damage is hard to realise, until the owner doesn't have to take loss following a real security event. Thus also the regulation of law is needed, which makes utilising of some security measurements obligatory without respect to the intention of the system owner.

The 410/2017. (XII.15.) Government order [7] prescribes the obligatory preparation of risk analysis regarding their work, to every financial organisation providing digital service. In case of default, official penalty can be played on them.

Risk management of governmental and local authority organisations

The „preliminary and posterior leadership monitoring inbuilt to the process" (PPLMP) regarding the financial activity of state hold organisations is defined by the Law CXCV. of 2011. and the 368/2011. (XII.31.) Government order on its execution, furthermore by the 187/2016. (VII.13.) Government order on control system and inner control of state hold organisations. According to the latter: *„Risk analysis: objective method to pick the fields to be controlled, which defines the risks within the inner control system of the activity of state hold organisation."*[8]

Thus the most important is, that the organisation has to define and measure risk in all the fields of its activity. Standard work of activity is bound to status, field of work, and personal responsibility. The analysis (PPLMP) has to be executed in each calendric year, it has to be learned by the responsible persons, and verified by the leader of the organisation.

The system of PPLMP defines the dealing with the following risks:

Risks from the outside that can hardly be decreased:

Infrastructural: Insufficiency or malfunction of infrastructure can interfere with normal procedure.

Financial: Negative effect of inflation on household precalculations.

Law and regulation: Rules and other regulations can narrow the coverage of the desired activity. Regulation can involve insufficient boundaries.

Political: Change of government can rewrite the goals set, or priority of them. A problem with a market deliverer can be of negative effect on the plans.

Natural disasters: Fire, flood or other natural events can be of an effect on the ability to fulfil the desired activity.

Financial risks

Household: Resources at hand aren't sufficient to execute the desired activity. Distribution of resources cannot be affected directly.

Financial: Loss of assets. Resources aren't sufficient for the desired avoiding measurements.

Operational risks

Operational-strategic: Following the wrong strategy. Strategy is based on insufficient or not precise information. Goals, that cannot be reached. Goals are reached only partially. Information: Not sufficient information to make a decision leads to a decision based on knowledge less than required.

Fame: In fame possibly appearing in the publicity can cause a bad effect.

Technology: The need to develop/change technology in order to keep efficiency. Technological breakdown can cripple the work of the system.

Project: Project-plan delivered without sufficient preliminary risk analysis. Projects aren't realised in time for the household or functional deadline.

Development: Missed development opportunities. Utilising of new approach without the sufficient analysis of risk.

Risks of human resources

Staff: The missing of personnel in sufficient quantity and quality restricts efficient operation.

Health and security: If the need of good mood among the employees doesn't get proper attention, the colleagues cannot fulfil their tasks.

Vital systems, critical infrastructure**:**

„65/2013. (III.8.) Government regulation on executing Law CLXVI. of 2012. [9] about the identification, appointing and protection of vital systems and facilities holds risk management connected to the protection of vital systems and facilities necessary. It defines risk analysis as follows:

„risk analysis: measuring of threat and risk factors to rate the vulnerability of the system elements, and the consequences of their jamming or destruction."

In my view this definition isn't clarified enough, it doesn't provide a clear direction to the measuring of risk factors. The regulation doesn't give obligatory rules on the methods of executing risk analysis, but it describes the way of identifying and measuring the risk in detail:

The regulation prescribes the creation of a list of risks threatening on all the system elements, then the clarification of the most probable reasons for these risks together with the expected negative outcome. While preparing the list of risks, one has to precede carefully, with attention to the vulnerability of the system elements. The regulation prescribes also the evaluation of each threat, further the dealing with them in accordance with the level of risk, although it doesn't define the means of risk analysis.

The outcome of the risk analysis has to be pictured in a so called identifying report. The operator realises security measurements depending on the type of risk analysis, and according to the level of risk, in order of the security of the system element.

In the Operator's security plan for vital system elements, the analysis of the most important threats and a risk analysis based on the vulnerability of each element and the possible effects have to be within. The regulation doesn't prescribe details, but in my opinion the monitoring of the information infrastructure of the system element is useful to be regarded as part of the universal risk analysis, and it is suggested to let the analysis of the field be done by an expert being home in this profession, and possibly independent.

Summing it up, it can be said, that the existence of risk analysis in regard of vital system elements is obligatory, however the regulation doesn't contain any detail on its content or methodology.

The regulation also mentions the vital system element within defence, and keeping the above rules is also regarding these system elements necessary.

Order of approach in risk management

Theoretical forms of risk management can be as follows:

Avoiding of risk

It means the general avoiding of certain damages and losses. It can also mean that the organisation gives its activity meaning the base of the analysis up because of the increase of risk. In the CRAMM type risk analysis a limit is defined above which the amount of risk cannot rise. If the risk cannot be decreased under the given level with any method, the part of the information system, that creates the given risk has to be demolished at the given place. Universal avoiding of risk, regarding every field is not possible, because that would mean the failure of operation in the analysed system. Abandoning of each service because of the high risk is possible.

Decreasing of risk

This principle means the real risk management, because here the organisation utilises own strategy of coordination, and own hardware-software assets to decrease risk. Measurements in this group can be divided into three parts.

Pre-loss principles secure, that the organisation works in an economic way, according to regulations. Universal security cannot be an aim, since that is virtually impossible. To this group belong the regular maintenance of buildings, machines, vehicles, and inventory, the use of redundant devices and networks, the protective system of thoughtful and professional operation systems, firewall, protection against malwares, processing of measurements and rules, picking, preparation and training of management and user personnel.

Pro-loss risk management doesn't care about avoiding the event of damage, since here the decreasing of the effects of realised damage is the point. Basic requirement is the refurbishing

of the system in the shortest possible time, by the fewest possible loss of data, with the smallest possible utilisation of material and human resource. It is important to keep the operationality stemming from the call of the organisation constantly up.

To the third category are belonging those risks taken, which don't require any action. In this strategic field, passivity is standard. These are risks which are negligible, irrelevant, but still don't fit into the first two groups. In some terminology these are called remaining risks, which the leader of the organisation has to agree with accepting on paper.

Sharing of risk, shifting of risk

In case of more organisations working together or outsourcing certain services, the risk taken is divided by all means. This can happen even based on a contract with assurance companies involved. Parties can be state organisations, officials, financial partners, investors or banks as well. The matching shaping of financial contract conditions can be one mean of shifting risk. When signing the contract, risk has to be measured, also the sharing of it among the agreeing parties. Assurance is also a form of shifting or sharing risk. [10]

International pattern:

ISO/IEC 27005: 2011 [11] pattern is dealing with the unification of information security risk analysis on international level.

ISO / IEC 27005: 2011 is helping the users in utilising the patterns of information security controlling system based on the risk analyses approach (ISO / IEC 27001).

Practical forms of risk management can be as follows:

There's regulation of law to prepare risk analyses in the field of public services. Because of this, many business companies are dealing with providing this service. Also software's have been developed to help the work of risk analysers. In the public sphere, and also at HDF the analyses is prepared by own colleagues, who, in lucky case have attended preliminary course on the possible means of execution. From the bulk of options I picked two strongly differing methods. Beyond these lots of other types exist. The followings were my choice, because the CRAMM method may be the best one according to the proposal of information security organisations, and the other type of analyses is also used in the public sphere, but not in the field of information security.

Gordon-Loeb Model:

To realize decreasing of vulnerability, Gordon and Loeb [12] proposed a very simple and general model in 2002. It is a mathematical economy model, which analyses optimal investment level in information security. With the aid of difficult mathematic calculations it shows, that the increasing of money going for information security activity of an information system to manage the vulnerability of the system isn't cost effective beyond a point. It defines the point to which it is affordable to go with turning material resources on the increasing of information security. The model puts requital aspects into focus.

According to the model, first the value of the protectable goods has to be measured from low level to high. Then the vulnerability of each system element has to be analysed from low to high. Then by comparing the two tables, the elements have to be defined, of which we want to decrease the vulnerability. According to the model, the protection of high value – middle vulnerability elements is providing a cost-effective, at the same time sufficient defence.

CRAMM[6] type risk analyses:

The method prepared by CCTA[7] is able to manage the risk of information systems firstly The practice of the risk analyses can be divided into three main groups of tasks, which comprise of further partial tasks.

[6] CRAMM - ***C****entral Computer and Telecommunication Agency* ***R****isk* ***A****nalysis and* ***M****anagement* ***M****ethod*

In the first group, the basic aspects are defined:

The scope of the risk analyses will be defined.

Asset elements of the system are identified and measured.

In the second group of tasks the risks are measured according to the proposed security requirements.

Identification of the threats meaning a potential danger to the system, definition of the type and level of each threat.

Analysation of the system's vulnerability, through which the realised threat can lead to a security event.

Comparison of the threat and vulnerability set, calculation of risk by multiplication, addition, weighting according to the decision of the analyser.

In the third group it is defined, above what level the risk has to be managed, also the counter measurements are described, whit which the level of given risks can be pushed below the level of toleration.

In information systems the most important value to protect is the data, which to process the system was created for. Basic features of the data, which have to be protected, are the confidentiality, intactness and disposability, furthermore, in case of network transmission, the credibility and authenticity. Evaluation of the risk analyses has to be done always according to the saving of the above features. It depends on the nature of contained data and the type of services provided by the system, which the features to be most protected are. In defence sphere generally confidentiality is the most important. In case of an education database, or electronic travel schedule, intactness and being authentic is the most important, confidentiality hasn't even to be secured since these information's are to be accessible to anyone.

SUMMARY

In the recent paper I collected the constant principles of maintaining electronic information systems in a secure way. I presented the main elements of recently operative regulation regarding this field. The possibilities, basic features, rules of creating risk management while planning, shaping and maintaining information systems, have been showed in particular. I presented that each organisation use different approach to analyse their risks. Occasionally also software's are used to prepare risk analyses, which can ease work, especially in case of large and difficult systems. But it has to be kept in mind, that any program isn't able to substitute human in maintaining risk management, experts from all fields have to be involved.

I clarified, that although there is regulation regarding information system security (ISO/IEC 27000:2011), none of these rules is universally obligatory, and they don't define the exact method of risk management.

In case of planning a new information system, especially if they have to process classified data, a preliminary risk analyses has to be done. The execution of this, in case of networks fulfilling public service is also an obligation defined by law.

In my view, among risk analysing methods, the CRAMM type is the most efficiently utilisable in case of information systems. It has been developed especially to analyse electronic systems. The lists of goods, threats and vulnerabilities can be useful, which can be prepared beforehand, according to the actual system. The calculation of this analyse are logical, they don't require high level mathematical knowledge like the Gordon-Loeb model,

[7] Central Computer and Telecommunication Agency (United Kingdom)

which can be a key feature to be considered if in a case of a new or broad information system, analyses has to be done at several places, and abilities and knowledge of the professional staff isn't equal either.

BIBLIOGRAPHY

[1] *Law L of 2013. the electronic information security of public and municipal services*.

[2] *Law CLV of 2009.on the protection of classified data*.

[3] *HDF 94/2009. MoD the Defense Ministry's information security.*

[4] *HDF 3/2012. MoD defining the general electronic security information requirements of the defense ministry and clarifying the security regulations*.

[5] *15/2017. (IV. 28.) MoD order on executing the tasks of the office providing control over defence aimed electronic information systems, and the electronic information security event managing system in defence sphere, and on the rules of executing voulnerability measuring.*

[6] PÁLINKÁS P.: *Kockázatkezelési eljárások alkalmazása az európai unió mezőgazdaságában,* PhD thesis [Szent István University, Gödöllő 2011 p.10.]

[7] *410/2017. (XII. 15.) Governmental order on providers of services to be reported*

[8] *187/2016. (VII. 13.) Governmental order 2. § l.*

[9] *65/2013. (III. 8.) Gov. order on the execution of Law CLCVI. of 2012. on identifying, appointing and protection of vital systems and facilities, 1. § 2.*

[10] SÁNDOR B.: *A Kockázatkezelés Jelentősége,* Economy College of Budapest, 2011. http://elib.kkf.hu/edip/D_15929.pdf (Date of download: 20.10.2017.)

[11] https://www.iso.org/news/2011/08/Ref1451.html (Date of download: 21.10.2017.)

[12] LAWRENCE A. G. and M. LOEB, professors at the University of Maryland (https://www.umd.edu/)