Neptun System Security Questions at Óbuda University

Viktória Katona-Kis
Óbuda University, Budapest, Hungary
kis.viktoria@rh.uni-obuda.hu

***Abstract* — The well-known Neptun Unified Education System is currently used by 44 higher education institutes. The system provides a complex solution for the universities, primarily in educational and financial administration areas. At the Óbuda University (the legal successor of Budapest Tech since 2010) Neptun has been first introduced in 2002 and is still being used. The database of the Neptun system at the university contains not only personal data of many students and instructors, but institute specific information on many educational, financial and other miscellaneous areas as well. The protection of sensitive information is essential, so the security of the whole system and the database connected to it also has a special role. Hereunder I will introduce the expected security requirements against certain components, as well as their practical implementations here at Óbuda University. As we can see from the results of the analysis, the adopted solutions provided an adequate protection in practice. However, while planning the future, besides the benefits, it is also important to consider the disadvantages and set the potential development possibilities.**

I. INTRODUCTION

The Neptun Unified Education System is currently used by several higher education institutes. The system provides the possibility of electronic administration in multiple areas and has been for many years. At Óbuda University (the legal successor of Budapest Tech since 2010) the system was first introduced in 2002 and is still in use today.

The database of the Neptun system at the university also contains sensitive data. The protection of sensitive information is crucial for the security of the system. Hereunder I will introduce the general properties and short history of the system at Óbuda University. I will also address possible safety issues in areas such as applied architecture, saving strategy, or other security features – all of which I examined. The human factor is also one of the most relevant factors concerning security. Besides reviewing the individual elements I will also take the current design and eventual weak points of the application into account. In addition to the above it is worth examining the necessity of future developments and possible development paths.

II. THE NEPTUN SYSTEM IN GENERAL

The first version of Neptun was published in 1997. This system differed from the current version not only in its appearance and structure, but it used completely different ideas and technologies in the background. In the beginning the users and even the developers struggled with several functional anomalies. The 'Neptun.Net' system started its operation from September 2005 as the enhanced version of the so called „Neptun 2000" and it is still being used today. Over the years the developer (SDA Informatics Plc. and SDA Studio Ltd.) – with the cooperative help of the educational institutions – has been shaping the Neptun system into a product that always tries to meet the constantly changing legislations, technical challenges and the ever-changing needs of its users. Neptun 438 is the current version being used by the all of the educational institutes and their students. It is important to emphasize that the system itself is the result of Hungarian development and execution, therefore the related references are only available in Hungarian.

The Neptun Educational System can be used in several areas. It is applicable to, but not limited to arrangement of educational and financial administrations, supporting different educational management tasks, management of facility and human data, and helping with fulfilling the institutes' reporting obligations. Beyond the above it is also capable of preparing and organizing large amounts of data according to institute requirements with the help of integrated and complex filters and queries.

Basically, the Higher Educational Institutes would be the users of a framework that can be shaped to their own individual needs depending on the local circumstances. This is made possible by the parameterization and the modular structure of the system. The disadvantage of the framework is that the universities practically get a ready-made application, which in fact can be parameterized, but is not developed completely based on the institution's needs. Operational problems that we have had while using the system in practice can be devided into two major groups: problems with the frameworks and problems related to institutional specifications and misconfigurated solutions.

The system is currently used by 44 institutions across Hungary. The illustration below gives an overview of this. Regarding the whole country this is a remarkable market share, although we can not mention real competitors on the market due to the nature of the product. To mention some larger institutions: Corvinus University of Budapest, Budapest Business School, Budapest University of Technology and Economics, University of Debrecen, Eötvös Loránd University, University of Nyíregyháza, University of West Hungary, Óbuda University, and Pázmány Péter Catholic University [1].

Figure 1. Neptun system user institutions in Hungary [1]

This illustration shows that 44 institutions decided to use Neptun, which is a huge success. Since so many different institution requests were kept in mind while developing the software users may come across interfaces and features that they may not necessarily need, as with all new software. However, in some cases there are features recommended by one institute that can be successfully used by others, too.

NEPTUN SYSTEM AT ÓBUDA UNIVERSITY

The Neptun System was first introduced in 2002 at Budapest Tech, the legal predecessor of Óbuda University. Budapest Tech was the very first among the domestic higher education institutions to introduce Neptun's subsequent version, Neptun.Net in September 2005. Starting from January 1st 2010, the school uses the system under the name Óbuda University.

During the 10 years of usage, the university tried to model the organizational and educational structures in Neptun. In order to achieve this, it defined the custom adjustable parameters and institute-compliant values of the code entries and implemented these in practice. As a result of different adjustments, they created a system that fits many established rules, and ensures the different processes work according to these rules during user activity in the system.

Additionally, each university can choose from many different available modules depending on what specific tasks it wants the system to become suitable for. The following illustration shows the currently available modules and also the interfaces that can be connected to the system.

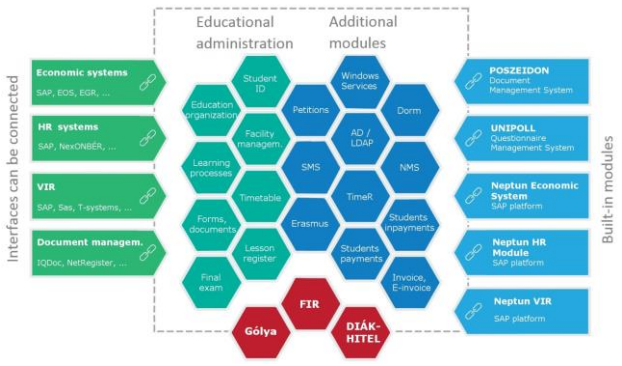

Figure 2. Interfaces and modules [2]

Some of the modules are published for the institutes by the developers as an integrated part of the system, such as teaching arrangements, invoices and prints management. Other modules are available as a result of individual developments based on the specific needs of institutions. Of course, not all of the accessible modules are utilized in practice, but continually build connections with the economic system and communicate with the Gólya, Diákhitel and the FIR (Higher Education Information System), and are necessary to complete the tasks arising during the academic year. The Poszeidon file and the document management system which has a common database with Neptun has also been used for years by the staff of the university.

Many modular developments are made based on user requirements, but the system has to ensure that the ever-changing legal-environment is followed by the institutions in practice. The Higher Education Information System operated by the Educational Authority is a good example, which is an electronic authenticity register to which higher education institutes are required to provide information. The required information is specified in the Higher Education Act No. CCIV. of 2011 and the Governmental Decree No. 79/2006. (IV.5.) [3]. In order to ensure the fluency of providing data as required by the statutory regulation and to keep the ability to manage desired tasks, the educational system had to grow and evolve in this direction.

From the list of connectible interfaces we must highlight the connection with the economic system: it gives an opportunity for the institution to administer the students' study-related financials. Through the Neptun, system students can handle their payments incurring in connection with their studies, download the invoice related to their payments and track the scholarship referred to them. The Hungarian state treasury transfers the bank statements to the university electronically with the help of the MÁK Electra program. The statements are imported into the Neptun system through an encrypted connection every day except for bank holidays. Every file and issued invoice created in the Neptun system is transferred to the financial office where they will be imported into the MÁK Electra or EOS financial system.

With time, beyond the content and functional development the technical background and procedures of the system have also been developed and optimized. You can find detailed information on this subject in the security questions section.

III. SECURITY QUESTIONS

The security issues of an IT system are determined by the components that it's made of, the environment that it's in, and the rules that it has to follow, as well as it has to take into consideration what kind of backup strategy is used by the institution. Regarding information safety analysis confidentiality, invoilability and availability are the most important aspects. We can examine the organizational, physical and logical security, within this topic [4]. In addition to this, other factors might affect the safety of the system as well, such as access management settings, security components (VPN, electronic signature), or even the users themselves.

System architecture is determined by the tools that are available for development as well as the organization's IT

strategy is an important factor which will be translated into action during practical execution. In similar environments like Neptun you find an important cornerstone and that is the specific data model that is used [5, 6]. Therefore, the need for continuous improvement in this area, both in terms of technology and design should continually be emphasized.

ARCHITECTURE AND BACKUP

The basic structure of the Neptun educational system that is currently in use at Óbuda University is built of the following elements: client layer, transfer layer and server environment. This way, the educational system in use is actually made of multiple (up to 4 or 5) separate parts. The simplified schematic below shows this layout:

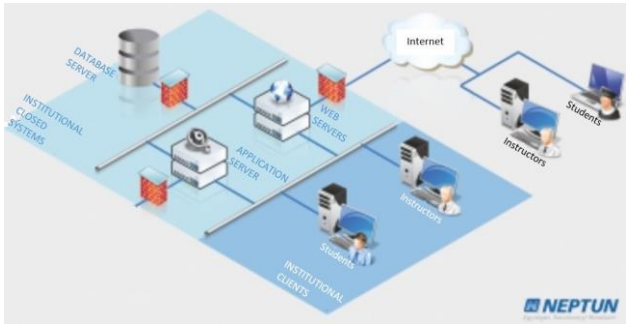

Figure 3. The Neptun.Net system architecture [7]

In case of the Óbuda University the following components can be distinguished:

- Oracle database server
- Application Server
- Web servers
- Hardware Firewall
- Software load balancer

Energy supply and communication lines between these components had to be provided redundantly as that is the basis of high availability. Hardware-based firewalls are designed to only allow validated traffic through to the internal network of the university. All of Neptun's components are located in this network as well.

Physical access control and physical availability are also very important parts of the technical protection methods. Physical protection of the system's assets is ensured by an access control system that is supported by strict eligibility rules. Availability is crucial in regard to the educational system in general, as it is essential for daily business and administration, fulfilling incoming requests of university students and staff through the web interface. For these reasons the server rooms are designed to protect the devices. As an example, the setup of cooler systems, the uninterruptable power supply, or the fire protection devices are all means of protection.

In the past Neptun was using a completely different set of tools and even a different architectural design at Óbuda University. Employees were able to work directly on the server with the help of remote desktop connection and web interfaces were supporting this process as well. The disadvantage of this design was that multiple users working on the server at the same time, using the same application at the same time, were slowing the server down significantly. Also overloading the network resulted in slower communication, or - in certain periods – unavailability on the web. Developing the communication channels was absolutely necessary along with rethinking the Neptun system as a whole. Currently all administrative users have to install a client software on their own PC that only communicates with the server if a specific request has been made. On one hand, this accelerated the processes, on the other hand this was a leap forward in terms of safety as well, because the communication channel became more closed.

Besides of fluctuating loads that are typical for the area of education, we also have to pay particular attention to handling the increased traffic during peak seasons, such as half term or exam periods. As for the most recent developments regarding Neptun, the university implemented a new, more effective technical device and introduced advanced virtualization procedures. The HP BladeSystem meets all today's IT requirements and in terms of its resources it exceeds the previously used dedicated servers significantly.

Moving of the complete Neptun educational system to a virtual platform – including web servers, database servers, and application servers – started in 2009 at Obuda University. With the introduction of the new layer, the system became more flexible and more scalable while availability and resource management were also stabilized. Besides the above, the VMware virtualization layer guarantees the improvement of fault tolerance in the physical layer. This way the main components of the Neptun system will be able to offer continuous multi-site operation, preventing possible hardware errors which can result in a system downtime. Another advantage worth mentioning would be that if an overloaded period is to be expected, the virtual web servers can be cloned to be able to keep up with the higher demand and simultaneously received requests. Also, the already existing resources (CPU, memory) can be changed dynamically. With the new tools we can optimize the settings of the power- and cooling systems, reduce operating costs, and by using virtualization methods, we can save valuable energy and hardware resources because we can run multiple virtual servers on a single physical server – thus, outside of the network they appear to be just regular physical servers. Óbuda University is a pioneer among the institutions of higher education in terms of introducing virtualization technology and it swiftly responds to all the new demands and challenges.

A non-negligible element in terms of security, the client program to log on to the system by adding their own user and password entry process is possible only through a VPN. The connection can only be maintained by using a so-called RSA-key (which is an encryption method) that can only be requested from and approved by the top management. In a so-called virtual private network Internet access is maintained through a VPN tunnel. A VPN is basically an encrypted connection, which grants the database a higher level of security. A further advantage is that by using VPN colleagues can access the client software securely even from a home based computer. The university recognized the importance of secure access very early, but did not at the time use the Neptun system currently in use in all institutions of higher education organizations. Web accesses are also only available through encrypted connection, using the "https" protocol that ensures that web communication can be

encrypted and authenticated. When it comes to the topic of backing up the system, institutions are doing everything possible to avoid a situation when they'd need a backup in practice, however, elaborating a proper backup strategy is one of the key elements of any IT system. There were some significant changes in this area at the university during the last couple of years. The early routine of weekly backup has considerably improved by now. In a week's period the system both works with daily backups, and comprehensive backups for the last three days on Wednesdays and Saturdays, as well as it starts the preparation for a weekly backup on every Sunday.

The simplified process is shown schematically in the figure below.

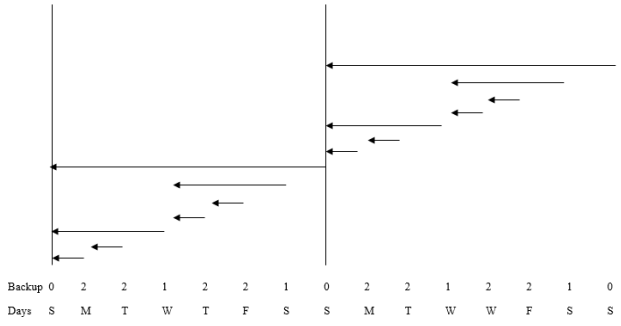

Figure 4. Backup process at the Óbuda University

Besides the backup itself, the storage of the saved data requires a prudent execution as well. In this particular case, the backed up data is stored at three different locations: first of all, it is stored on the server itself, as it always contains the backups of the previous two weeks. Also, it is stored on a physically separated and elsewhere located backup server, as well as on an external drive. In practice, many institutions face storage problems. It could be a solution to have a regulation for organizing encrypted data storage on a mutual basis with other higher educational institutions. The question of proper backup is a delicate issue – although an institution can have the relevant data when their backups are verified, still, the most relevant concern is whether this data can be brought back in a potential emergency situation.

There are plenty of expectations that IT systems should meet. Among other things, they should be cost effective, upgradeable, provide high availability, proper efficiency [8, 9] and comply with safety rules. In the last couple of years these expectations have shown to be very different due to technical and systematical developments. Of course, expectations also vary depending on who we ask: the institution, IT professionals or the users themselves [10].

AUTHORIZATION MANAGEMENT

Authorization management is related to the subject of security. The authorization system of Neptun.Net is based on roles and functions and this helps us to set up the authorization system according to the systematic structure and its regulations. From a security perspective it is a relevant fact that we can determine a very detailed set of permissions to each user – enabling them to access, change or even add data. Setting the user's roles helps them to understand the system better because they would not see the whole menu structure, only those parts would be visible for them that they need for their own work, specifically. This, on one hand quickens the working process, on the other hand reduces the possibility of mistakes and mishandling of data [11].

Óbuda University expressed its need for the improvement of the authorization system in 2009, and at that time started designing individual roles satisfying individual needs. Thanks to this early realization, a university – given the appropriate authorization level - is allowed to decide on its own whether the buttons to certain menu items are visible or useable for users.

Óbuda University uses the following main roles at present:

- Student: this role enables access to the student's web interface.
- Instructor: this role enables access to the instructor's web interface, and is essential for uploading any data in the instructor's department.
- All students: this role enables insight in certain student information, but is not permitted to implement any changes
- FIR data management: many roles were created over the years upon an increasing number of requests. The authorization for FIR data management is one of these. Since higher education institutes have by law a reporting obligation to FIR, this role enables the related tasks to be completed.
- HR Admin: this role enables any human resources data to be created and edited
- Student residence admin: this role enables the registration and administration of any data related to the student's residence
- Timetable creator: at the Óbuda University this role enables the users not only to create their own timetables but they can also access facility management data closely related to their tasks.
- TO administrator: this role is typically used by the educational department. It enables them to view and edit the data of the students assigned to them, while they cannot view or only have limited access to the data of other students. At Óbuda University as a result of multiple combined roles, an extended authorization is ensured for the educational departments in order for them to fulfill their duties also regarding administration of student cards and handling of diploma supplements.
- Academic Department admin: this role enables the user to view all the subjects of the establishment but is only able to edit the subjects of its own institute.
- Faculty administrator: typically this role is owned by the Neptun system administrator of each faculty. This permission covers the roles of the educational department and the academic department, furthermore it enables its user to view, create and edit data under several menu items on a faculty level.
- System administrator: this role does contain the authorizations of all of the above, extended with certain additional menu items and interfaces.

The design of the authorization system follows the organizational structure of the university as it ensures separate roles for the staff of educational departments, faculties, institutes and to the administrators who handle the whole system comprehensively.

ELECTRONIC SIGNATURE

In Hungary, the legal background of accepting electronic signatures on official documents is given by the Act 2001. XXXV. Since we joined the European Union (May 1st 2004) it is even possible to issue an electronic invoice, that is to be considered equivalent to a paper-based one.

Neptun.Net includes an electronic signing module that is certified by MELASZ, the Hungarian Association of Electronic Signatures. Developers of Neptun.Net can guarantee the authenticity of the documents given by the system thanks to electronic signatures and timestamping [7].

Óbuda University uses the possibility of electronic signatures on two fields at present. Within the accounting department, with organizational signatories, and when communicating with FIR, using personal signatures. When issuing invoices, the electronic signature identifies the organizational signatories while their authenticity is certified by the timestamps and the certifying editor. The advantage of this procedure is the rapid decrease of production costs and time, while issuing the documents and sending them out can also be automatized if required. It is an interesting experience we made with our invoices sent to partner companies. The authenticity of the invoices is often questioned since despite of today's advanced technologies, this type of verification is still little known.

Data that are supposed to be sent to the Higher Education Information System, are sent in XML files, by so-called data containers. At this point for instance, the safety of the forwarded data can be a delicate issue. It will be ensured by the cooperation of the Education Office, the universities, and the developers of the educational systems. One of the main principles of the Education Office is the respect of authentication by electronic signatures in disclosed data [12]. In fact, FIR has three communication channels to every institution - the data will be received in classified containers and the feedback to the institutes will also be given through these secure channels. While receiving the containers, there are multiple checkpoints that have been implemented in the procedure. One of these checkpoints is the inspection of the electronic signature because only those data packets can be acknowledged that have the signature according to the legal requirements. On one hand it is verified whether the digital signature is authentic, on the other hand its validity is examined by the verifying service that issued the signature in the first place. It will be confirmed, as well, whether the person providing the data to FIR was authorized to do so. At last, the certificate of the digital signature that is provided by the institutions will be compared to the signature in the containers [13]. As a result of the above process the containers of data will be either be forwarded for further processing or denied.

Overall we can conclude that it was useful for the university to implement the use of electronic signatures because this can be the basis for a more economical operation, the lead time of certain documents can be decreased, and a more structured and clear environment can be provided to both the issuing and the receiving parties.

THE HUMAN FACTOR

Even if an institution uses the most advanced technologies and softwares in order to properly control the access to specific data, the human factor is still inevitable [14]. In a security system consisting of the most advanced technologies the weakest link is always the person controlling it [15]. The people are those who manage and interpret the informational sources and in case of their failure they can cause intentional or accidental damage to the organization. In order to efficiently handle such situations it is an essential step to implement and maintain an Information Security Management System [16]. It is also important to develop a security culture that gives every organizational member joint and severe liability to maintain safety. It is reinforced by a security-consciousness, in which the individual risk perception goes beyond personal security threats and extends into an organizational level [17].

It is particularly important that the university administrators manage data with awareness concerning that since 2002 more than 65000 student-records, nearly 2200 employee-records and more than 28000 course-related records have been entered into the Neptun System's database. The size of the database is currently about 830 GB. In addition to the large amount of records secure data management can also be affected by the complexity of the whole system. The more menu items, interfaces and functions exist, the more diversified the system is, and necessarily the more difficult it is to use for the users.

Compared to the initial period more and more functions have been implemented in the Neptun System, which is beneficial in a sense that more and more administrative tasks can be done at one place, but on the other hand it raises the issue of complicated managment. This constant improvement can be a big challenge both for the users and the developers.

The most efficient means of reducing safety threats caused by the human factor is training [18]. Without proper training users will not be able to use the system unrestrained, confidently and safely, that may result in faulty or unnecessary data recording or even in data loss. Óbuda University is trying to put great emphasis on training and making it available to all users, via individual training materials, comprehensive annual lectures, smaller group consultations on specific areas and user support services. The precise and detailed regulatory system consistently sets the work policy procedure of the system in a clear and understandable manner. In addition to all this it is also important for the organization to have the latest information that can be obtained for the particular areas from the Educational Authority and from publications by Neptun's developers or by attending various workshops.

In addition to the different trainings and user manuals, developers can help the users to understand the system and use their products confidently. Creating a logical structure, a user-friendly interface and integrating some additional safety features (warning popups, feedbacks on trouble tickets) may as well help to a certain extent. The ergonomy of a software often shows a correlation with its development. It can be the key to an efficient development if the potential users are getting involved at an early stage of the development [19]. The proper qualification of the

developers and the high standards of the development and product support processes are also important. These are guaranteed by a TÜV Rheinland certification in accordance with ISO 9001.

The ability to view modification-history has proven to be useful in practice. Basically, it means the logging of the modifications that can be viewed by the users on each page based on their chosen data. It is useful on one hand because it clearly shows who, when and how modified a specific record, while on the other hand it also increased the users' sense of responsibility while working on data stored in the system. It has not been mentioned yet, but the passwords used in the system are also a major issue. A password-authentication is required every time a user logs in the thick client and the web-interface. It was not a general practice to set criteria and requirements for given passwords, but it is more and more common these days. It would be useful if teachers even at basic educational institutions would emphasize the importance of choosing a safe and well-considered password [20]. It is a primary requirement that only the user knows the password, plus the length and the characters used (uppercase, lowercase alpha- and numeric characters) can also be specified.

It is also recommended to store passwords encrypted, change them regularly, log unsuccessful intrusion attempts and block them after a specific number of cases. From a security perspective it is also useful to interrupt connection after a given time period of inactivity [4]. Although the institutions are not allowed to customize password-requirements according to their own needs, the passwords are stored encrypted in a 64bit database. In practice the web interface also terminates the connection after 5 minutes of inactivity. A live VPN connection is mandatory to connect, which requires a separate username, password and an RSA key.

Of course, the human factor plays an important role in this sense as well, since responsible handling of passwords and workstations again depend on the user. Users are chosen from different groups: administrators, instructors and students also use the system. Security awareness is important in all groups for example regarding passwords. The mostly technical training profile of the university can help in this, together with the precise technical attitude of instructors and students using the system, often associated with this field. The examination of this question can provide an interesting base for further researches, however a previous research (based on a different subject) came to a conclusion that a student's faculty (e.g. economic or technical) does not influence the security awareness [21].

CONCLUSION

The above shows that although it is not a business environment, a University Educational System may also raise several security questions. Keeping up with the technological development plays a key role among many others in the stability, availability, resource management and responding ability of the system. In this aspect informatics have always come into conflict with management since the latest technologies are expensive. IT professionals often prefer to replace apparently fully functional devices just to keep up with the latest system improvements. By fully utilizing its limited resources Óbuda University has always tried to put a great emphasis on development of meeting the highest expectations.

Besides the technical details, equipment, softwares and processes the human factor also plays a key role in terms of security. Users often do not realize their responsibility for keeping their passwords or other sensitive data safe. There are various tools to develop this, the most effective ones in academia to highlight their individual responsibility are the various trainings, rules and on the secure usage of systems. By raising the security awareness and using the appropriate tools it can be an important target ofestablishment and maintenance of the organizational security culture.

REFERENCES

[1] SDA informatika, „Neptun Egységes Tanulmányi Rendszert használó intézmények," Downloaded from: http://neptun.org.hu/neptun-egyseges-tanulmanyi-rendszert-hasznalo-intezmenyek/, Downloaded on: 20.10.2015

[2] SDA informatika, „Interfészek és modulok," Downloaded from: http://www.sdainformatika.hu/Home/Neptun, Downloaded on: 20.10.2015

[3] Oktatási Hivatal (2012), „Felsőoktatási Információs Rendszer (FIR)," 22.08.2012, Downloaded from: http://www.oktatas.hu/felsooktatas/fir/fir_mukodes_alkalmazas, Downloaded on: 22.10.2015

[4] L. Horváth, Gy. Lukács, T. Tuzson, Gy. Vasvári, Informatikai biztonsági rendszerek, KVK, Ernst & Young, Budapest, 2001

[5] P. Szikora, "Measured Performance of an Information System," 7th International Conference on Management, Enterprise and Benchmarking, Budapest, 2009.

[6] A. Keszthelyi, "The Role of Data Modeling in Information System Efficiency," 2nd International Conference for Theory and Practice in Education, Budapest, 2009.

[7] SDA informatika, „A Neptun.Net rendszer architektúrája," Downloaded from: http://www.sdainformatika.hu/download/Neptun.Net_Egyseges_Tanulmanyi_Rendszer_tajekoztato.pdf, Downloaded on: 20.10.2015

[8] A. Keszthelyi, "How to Measure an Information System's Efficiency?" In: Gy. Kadocsa (ed.) MEB 2009 – 7th International Conference on Management, Enterprise and Benchmarking, Budapest: BMF, 2009. pp. 213-219.

[9] A. Keszthelyi, "Remarks on the Efficiency of Information Systems," Acta Polytechnica Hungarica Vol. 7, No. 6, 2010. pp. 153-161.

[10] S. Cramm, IT-frusztráció. Akadémiai Kiadó, Budapest, 2012

[11] A. Keszthelyi, P. Michelberger, "From the IT Authorisation to the Role- and Identitiy Management" In: A. Szakál (ed.), 4th IEEE International Symposium on Logistics and Industrial Informatics: LINDI 2012. Smolenice: IEEE, 2012. pp. 173-177

[12] Felsőoktatási műhely (2015), „Felsőoktatási Információs Rendszer," 08.01.2015, Downloaded from: http://www.felvi.hu/felsooktatasimuhely/fir, Downloaded on: 10.22.2015

[13] Oktatási Hivatal, FIR füzetek 5., „Adatbetöltési folyamat a FIR-ben.," Downloaded from: http://www.felvi.hu/prot_bin/hivataliugyek/fir/szakmai_anyagok/FIR_fuzet_05_adatbetolt.pdf, Downloaded on: 22.10.2015

[14] Gy. Lukács, J. Kerekes - et al., Információ – biztonság. Cedit Információtechnikai Kft., Budapest, 1997

[15] A. Keszthelyi, „Paradigmaváltás – Biztonság – Emberi Tényező," Taylor Gazdálkodás- és szervezéstudományi folyóirat, 2015. vol. 7., 1-2., pp. 406-412

[16] P. Michelberger, J. Beinschróth, G.K. Horváth, „The Employe – An Information Security Risk," Acta Oeconomica Universitatis Selye, 2013. 2: (1), pp. 187-200

[17] K. Lazányi, „A biztonsági kultúra," Taylor Gazdálkodás- és szervezéstudományi folyóirat, 2015. vol. 7., 1-2., pp. 398-405

[18] Cs. Kristóf (2013), "A britek a biztonságtudatosság növelésére költenek," 06.25.2013, Downloaded from: http://bitport.hu/biztonsag/a-britek-koeltenek-biztonsagtudatossag-noevelesere, Downloaded on: 10.25 2015

[19] L. Izsó, M. Antalovits, Bevezetés az információ-ergonómiába. Emberi tényezők az információs technológiák fejlesztésében, bevezetésében és alkalmazásában. BME Ergonómia és Pszichológia Tanszék, 2000

[20] A. Keszthelyi, „About passwords," Acta Polytechnica Hungarica, Vol. 10, No. 6, 2013. pp. 261-268

[21] P. Fehér-Polgár, „Felsőoktatásban tanuló hallgatók biztonságtudatossága," Taylor Gazdálkodás- és szervezéstudományi folyóirat, 2015. vol. 7., 3-4., pp. 15-21