Advances in Economics, Business and Management Research, volume 138
2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)

Development of Students' Digital Competences When Studying the Functional Capabilities of Modern DLP-Systems

Shabalin A.M.[1] Kaliberda E.A.[1] Kaliberda Yu.E.[2]

[1] *Omsk State Technical University, Omsk 644050, Russia*
[2] *ITMO University, Saint-Petersburg 191101, Russia*
**Corresponding author. Email: sham.omsk@gmail.com*

ABSTRACT
In the paper, the specifics of training future information security specialists, who are needed to have a formed competency for neutralization of internal and external information security threats are being analyzed. According to the authors, all kinds of corporate information and personal data leaks arising from the actions of so-called "internal intruders" or insiders represent a particular danger, against which the Data Loss Prevention software class (DLP systems) is the most effective remedy. InfoWatch Traffic Monitor 6.11 is a Russian software product certified in Russia FSTEC system and considered as one of the world leaders in this class of software. Based on the license obtained from InfoWatch, in the virtual laboratory of Omsk State Technical University a specialized stand was created, which gives an opportunity to develop one of the most important and modern digital competencies - "Corporate protection from internal threats to information security". Using it as a basis, students gain skills to configure and verify the DLP system, determine security policies, ensure control of information flows in the company and analyze incidents that have been identified. For this purpose, an algorithm for introducing a DLP system into the educational process have been developed, where students could define information security objects and develop appropriate policies to prevent data leakage and identify possible incidents, intercepts confidential information through controlled communication channels.
Keywords: *competency formation, digital competencies, corporate protection, information security, internal threats, insider, DLP-system, InfoWatch, virtual laboratory*

1. INTRODUCTION

In modern education a concept such as "skills" has appeared denoting the basic skills or competencies of a graduate, which can be divided into "hard" and "soft" [1]. The former indicate knowledge of the profession, the latter indicate the ability to work in a team, communicate, present achievements, etc. Both types of competencies are undoubtedly important for a university graduate, and nevertheless, recently experts have talked about the necessity of "digital skills" – a set of skills that modern specialists need in their work connected with the digital network economy [2]. According to the Networked Readiness Index (Networked Readiness Index is a comprehensive indicator characterizing the development of information and communication technologies level in the countries of the world), proposed by the World Economic Forum to assess countries'
digital economy preparedness, Russia ranks 41st among other states [3].

The digitalization of education, including high education, is considered in different contexts, but the development of digital skills is a key moment to preparation on different education levels which allows to create a full member of society ready to work with network digital technologies that the 21st century brings to the modern economy [4, 5, 6].
Digital skills can be examined depending on the direction of study, either "hard skills" if these skills are professional for the student or "soft skills" if they are considered from the point general educational competencies of view [7, 8].
In our opinion information security related precisely to the field of professional activity since everyone, both specialists and ordinary users whose activity are not directly connected to information security should have specific skills to work with information safely [9]. For specialists in information security the ability to resist internal and external threats is undoubtedly hard skills; for other specialties information security is considered as soft skills since they do not have to understand all the details of the fight against malicious software, but they must be literate in the information security field, know its basics and understanding about what can be done in various

situations to maintain the confidentiality, integrity and availability of important information.

This paper is focused on the training of specialists in the information security field which means that throughout the work digital skills are being considered professionally as hard skills.

One of the main requirements to the modern specialist in information security is the ability to solve real tasks regarding information security of business processes and organization management [10]. Information security that is "torn off" from business have no meaning nowadays.

A modern analysis of information security threats begins with their classification and identification of the most frequent ones. Currently the information security theory has several classification options, among which the most popular is the division by sources of information threats into external and internal [11].

In the recent past an external attacker (hacker) used to be considered as the main threat and for many years companies have been struggling with unauthorized access and protection from outside intrusion has achieved significant results. Nowadays breaking through the company' external protection becoming more and more complicated so the necessary information might be obtained from a company employee who has successfully authenticated and gained access to corporate information. Therefore the situation has radically changed and internal intruders (insiders) acting in accordance with personal motives sometimes become even more relevant threat to the company information security and every year the situation is aggravated.

Thus, for the first half of 2019 InfopWatch recorded 1276 cases of information leakage from companies which is 22% more than for the same period in 2018 (695 cases due to internal violators) [12].

Thereby since 2017 during the training of the specialists in information security, recommendations on the development of digital skill under the name "Corporate protection from internal threats to information security" among the students began to appear. This skill is aiming for protection from internal data leaks that occurred intentionally or by negligence through technical communication channels. Students should know the basics of corporate protection from internal threats, understand how to apply the regulatory framework to the incidents' classification and investigation and be able to use systems and methods designed to protect data [13].

From the digital skills' point of view future specialists in the information security field should be able to work with modern software systems protecting corporate information from internal leaks.

Leak detection and prevention systems (Data Loss Prevention, DLP-systems) appeared around 2006. Their work is based on the analysis of the internal traffic that exists in the protected network of the enterprise. A well-chosen implemented DLP-system can protect from negligence and erroneous actions of employees and prevent almost all possible scenarios of information leakage through internal channels [14].

Preparing students for work with modern DLP-systems is a technically complex process. In our opinion, it can be successfully organized and carried out only in a specially equipped virtual university laboratory [15]. Such a laboratory has been effectively functioning for two years in the Omsk State Technical University, Department of Integrated Information Security and it helps to solve a number of educational tasks in holding various disciplines connected with Informatics. However, it acquired the greatest importance after the creation of a virtual laboratory stand in it for the development of students' digital competencies while studying the functionality of modern DLP-systems.

2. BACKGROUND

2.1. Research methodology

At the Department of Integrated Information Security, Omsk State Technical University students are being trained in learning tracks:

- 10.03.01 – Information Security (Bachelor degree)
- 10.05.05 – Security of Information Technology in Law Enforcement (specialist degree)

In December 2019, the Russian company InfoWatch introduced the next version of its DLP-system InfoWatch Traffic Monitor 6.11. OmSTU received a license for the three main products of the company[16]:

- InfoWatch Traffic Monitor (IWTM) – the main component which is designed to analyze the traffic of the company' computer network;
- InfoWatch Device Monitor (IWDM) – a component for protecting workstations that has a server and client sides;
- InfoWatch Crawler – a component for controlling confidential information on network data storages.

To work with these software products, specialized virtual stands were organized in the Omsk State Technical University laboratory where students configure and check DLP-system, determine security policies, monitor information flows in the company and analyze incidents that have been identified, using modern technologies. The principle of stands operation is shown in Figure 1.

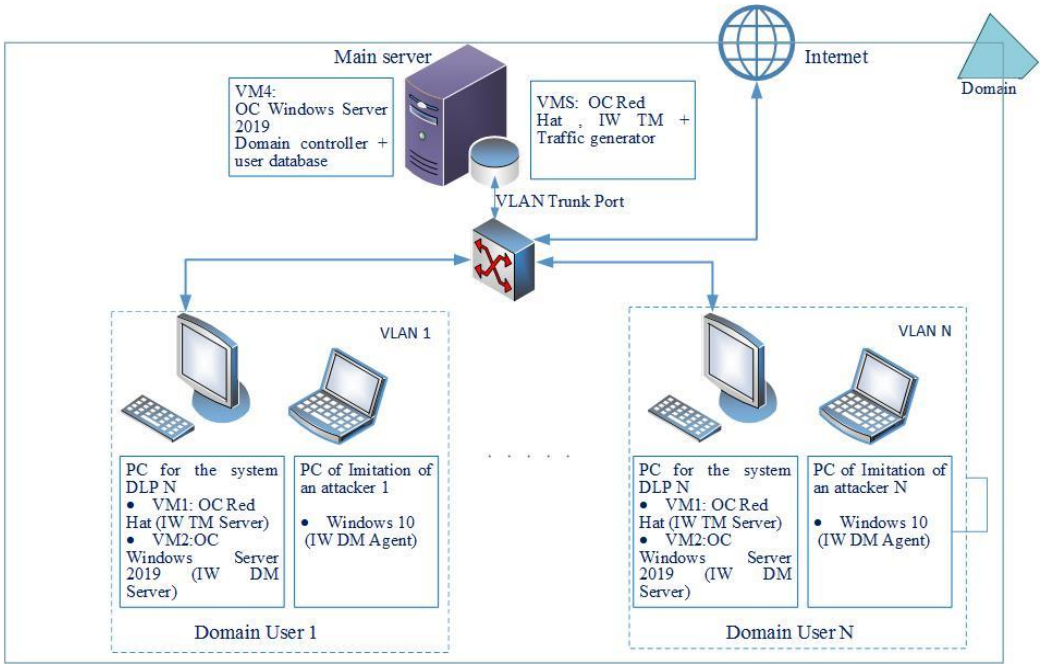

Figure 1 InfoWatch laboratory workflow

One of the two laboratory servers was chosen as the hardware platform: Dell PowerEdge R530 (2U/ 2xE5-2650v4 (2.2GHz/12Core/30Mb)/ 6x16Gb RDIMM(2400) / 8x4Tb SATA 7,2k/ DVDRW/ 4xGE/ 2x750W).

A RAID-5 disk array was organized on this server and the VMWare ESXi Server 6.5 hypervisor, which makes it possible to create a flexible virtual infrastructure in accordance with the needs of any organization, was installed.

Each stand can be simplified as a logical topology form which is represented in Figure 2 and organized on the basis of a standard personal computer with the VMware vSphere Client virtual machine manager to establish a local area network connection with VMWare ESXi Server.

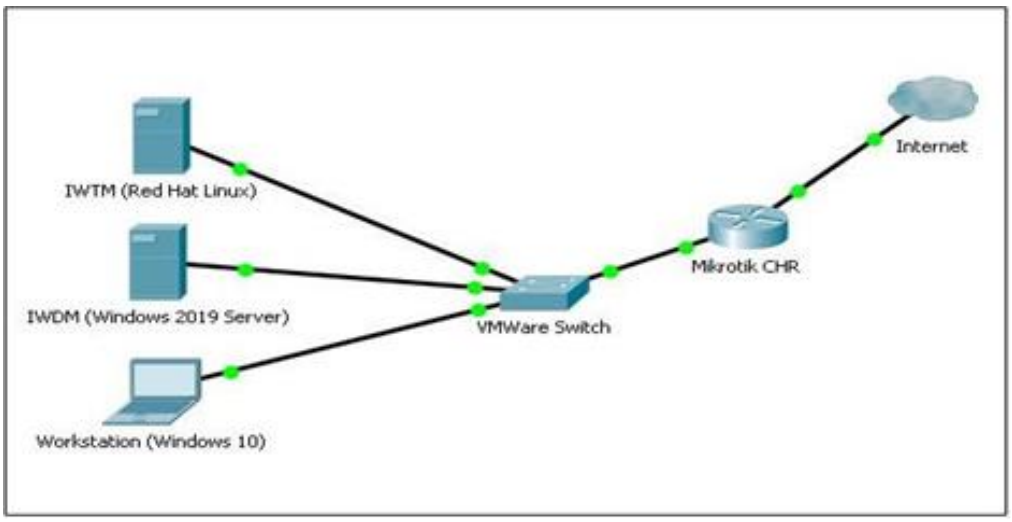

Figure 2 Logical topology of the developed virtual network

An infrastructure of three virtual machines, on which the InfoWatch Traffic Monitor software package is deployed, is created inside the hypervisor consisting of two IWTM and IWDM servers as well as a client computer from which insider actions are emulated.

All three computers are located in the same virtual local area network (VLAN) and are connected using the virtual switch VMWare Switch. Also they have an access to the

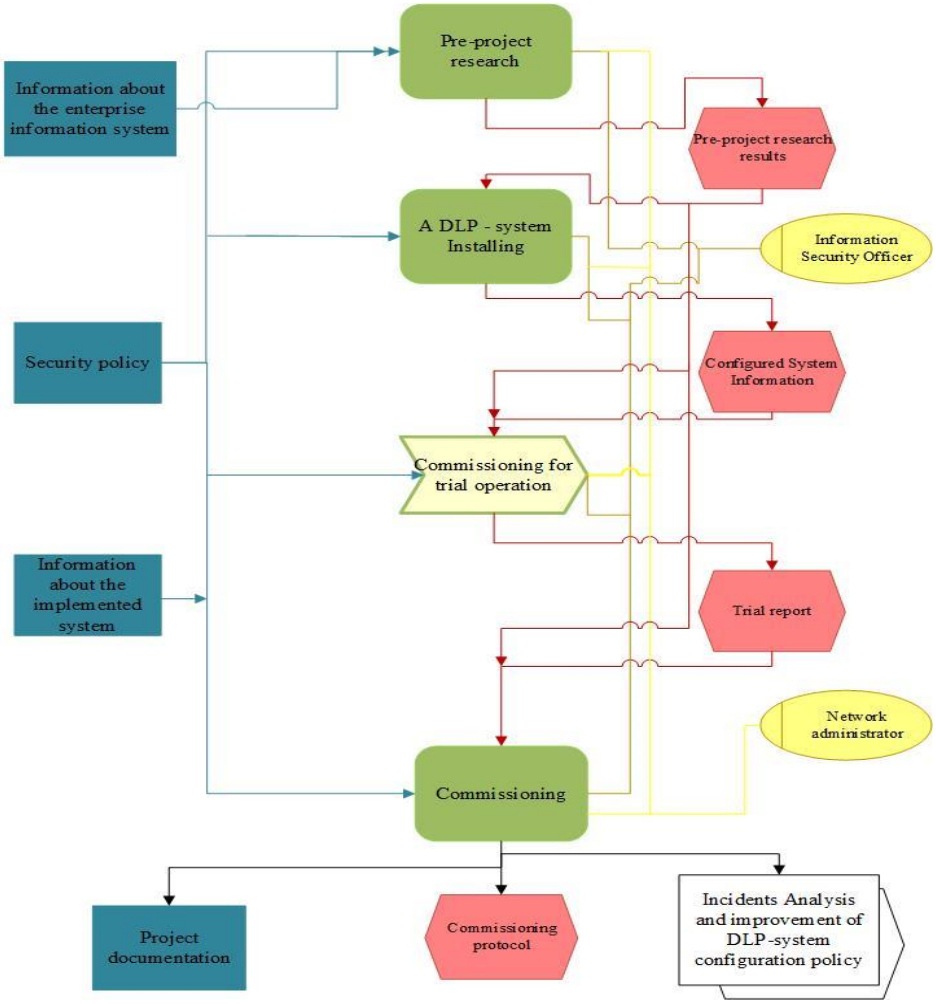

Figure 3 DLP-system

Internet via the Mikrotik Cloud Hosted Router (CHR), which is specifically designed for working in virtual environments on 64-bit platforms and can be used with most popular hypervisors, such as VMWare, Hyper-V, VirtualBox, KVM and others.

2.2. Research results

As a result, the students gradually carry out the following preparatory work on the virtual stands of the laboratory:

1. Install and configure:
   - Red Hat Linux operating system, Postgres DBMS, IWTM server;
   - MS Windows 2019 Server operating system, Postgres DBMS, IWDM server and InfoWatch Crawler module;
   - Active Directory directory service and DNS (Domain Name Service);
   - The client operating system MS Windows 10 under which the computer is entered the created domain, the agent part of IWDM is centrally installed from the server;
2. InfoWatch software products are integrated with Active Directory.

During the approbation of stands' work by students a hypothetical company, which provides desi gn, implementation, testing and maintenance of local area networks to customer enterprises, is being considered as an object of corporate protection from internal threats to information security.

The procedure for introducing a DLP-system into an integrated information security system of an organization should be carried out strictly stepwise.

The action algorithm developed by the authors of the article allows to streamline all actions and simplify the task of implementing a DLP-system. It contains 4 consecutive stages, all processes of which are implemented by students in laboratory work (Figure 3).

Figure 3 The process of implementing a DLP-system to the enterprise diagram

The first stage of the pre-project research is characterized by the presence of the following processes:
1. Conducting an audit of information security and risk assessment;
2. Creating a list of confidential information and a scheme for delimiting access rights to data;
3. Creating a legal framework for the implementation of DLP;
4. Calculating an economic efficiency of implementation;
5. Choosing an appropriate DLP-system and its configuration in accordance with the needs and resources of the company.

At *the second stage* of the DLP-system installation, the installation and initial configuration of the system are being made and a security policy is created based on the needs and activities of the organization.

At *the third stage* of the DLP-system trial operation, the following works are carried out:
1. Analysis of secured network channels and coordination of a set of technical documents describing the final design decision;
2. An inventory of data carriers and data paths that are threatened by unauthorized actions and on which the DLP-system will be installed;
3. Testing the performance of the system in real conditions.

The fourth stage of the commissioning process has the following components:
1. Training of specialists responsible for working with the DLP-system;
2. Analysis of the DLP system pilot launch (if necessary, additional system configuration with minimization of false positives);
3. Launching the system into commercial operation.

2.3. Results discussion

An outcome from performing all of the above actions is that students during the semester obtain a qualitatively functioning DLP-system. On the created virtual stand, they develop and test the following security policies for a hypothetical organization:
- The policy of reference documents interception;
- The policy of a category and term interception;
- The policy of a text object using regular expressions interception;
- The policy of a document with a reference print interception;
- The work of the "white" list of devices on client computers;
- The work of the "black" list of applications on client computers.

After applying these policies they intercept confidential information; the list of available external devices is issued to the user on the client computer and the software that is not allowed for use during working hours is disabled.

In addition, interceptions are carried out on various channels of confidential information sent by the user:
- Email via SMTP (Mozilla ThunderBird email client) and HTTP (web-mail);
- Screenshots and their automatic recognition using OCR Tesseract (additional software);
- Text messages - in Skype and Pidgin (via XMPP);
- Print events - on a local printer;
- Data copied to the clipboard;
- Data copied to an external device (USB Flash).

Furthermore, students detect confidential information in the user folder using the InfoWatch Crawler program.

At the final stage of work, students use the analytical functionality of the InfoWatch Traffic Monitor system to report on identified incidents and analyze the received data:
1. Organize a selection of events according to the created conditions;
2. Generate reports on the created conditions based on the data collected at the stand.

Thus, as a result of building and implementing a virtual model, students successfully develop the digital skill "Corporate protection from internal threats to information security": they test the functionality of the organization confidential data protection from leaks caused by illegal actions of employees (insiders) committed both purposefully and as a result of negligence or inattention. For a hypothetical organization, students identify relevant internal threats and leakage channels, determine confidential information and the stages of implementing a DLP-system to a company' work.

3. CONCLUSION

In the existing virtual laboratory, virtual stands were created on the basis of the VMWare ESXi Server 6.5 hypervisor where students test the functionality of the InfoWatch Traffic Monitor 6.11 DLP-system. This work on corporate protection against internal threats includes the assembly, installation, testing, usage and maintenance of specialized software and hardware systems for intercepting and analyzing data traffic circulating in the organization. In the DLP-system students create security objects and develop security policies that consist of appropriate sets of rules. Information security policies are applied in practice to block possible data leak channels and identify security incidents where filtering mechanisms are used in the intercepted traffic.

Thus, in our opinion, the construction of a model in a virtual laboratory for corporate information protection is an indispensable component of the educational process during studying DLP-systems for training future

information security specialists. Only thoughtful phased work based on a virtual model, created considering the needs of the enterprise, allows to apply security policies and verify their efficiency. Thereby, the necessary digital competencies of a future competitive specialist are developed.

REFERENCES

[1] Galazhinsky E, What is not taught at universities, Vedomosti, 2017, [e-resource]. https://www.vedomosti.ru/opinion/articles/2017/08/03/727760-ne-uchat-v-universitetah (date of reference 02.03.2020).

[2] Popova O.I, Transformation of higher education in the conditions of the digital economy, Management Issues, (5) 2018. DOI: https://doi.org/10.22394/2304-3369-2018-5-158-160

[3] Network readiness index. Information about the study and its results, 2017. [e-resource]. : https://gtmarket.ru/ratings/networked-readiness-index/networked-readiness-index-info. (date of reference 27.09.2018).

[4] Podolsky O, What digital competencies should the future personnel have? , National Technical Initiative, 2020, [e-resource]. https://ntinews.ru/blog/publications/kakimi-tsifrovymi-kompetentsiyami-dolzhny-obladat-kadry-budushchego-.html (date of reference 02.03.2020).

[5] Istvan Simonics, Digital competency in higher education, 2013 International Conference on Interactive Collaborative Learning (ICL), 2013, pp. 88-91. DOI: https://doi.org/ 10.1109/ICL.2013.6644542

[6] Tulchinsky G. Digital Transformation of Education, Challenges for Higher School, Russian Journal of Philosophical Sciences.(6) 2017, pp. 121-136.

[7] Gaivoronskii D. V. ; Kutuzov V.M. ; Minina A.A., Digital transformation of engineering education, Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations), 2017, pp. 3-6. DOI: https://doi.org/10.1109/IVForum.2017.8245954

[8] Hancock D, Effects of performance assessment on the achievement and motivation of graduate students, Active Learning in Higher Education, (8) 2007: pp. 219-231. https://doi.org/10.1177/1469787407081888

[9] Li Bian, Application of Digital Technology in Open and Distance Education, 2009 International Conference on Networking and Digital Society, (5) 2009, vol. 1: pp. 273-276. DOI: https://doi.org/10.1109/ICNDS.2009.74

[10] Vayndorf-Sysoeva M.E., Subocheva M.L., "Digital education" as a system- forming category: approaches to definition, Bulletin of Moscow State Regional University. Series: Pedagogy, (3) 2018, pp. 25-36. DOI: https://doi.org/ 0.18384/2310-7219-2018-3-25-36

[11] Skiba, V. Yu. , Kurbatov, V. A. Guide to protecting against internal threats to information security, Peter, St. Petersburg, 2008.

[12] Global survey of confidential information leaks in the first half of 2019, [e-resource], https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1. (date of reference 20.01.2020)

[13] Corporate Information Security: Current Skills of Digital Skills, [e-resource], https://worldskills.ru/media-czentr/novosti/informaczionnaya-bezopasnost-korporaczii-aktualnaya-kompetencziya-digitalskills.html (date of reference: 02.03.2020).

[14] Threats to information security: review and assessment. Comprehensive information security at the enterprise, [e-resource], http://rus.safensoft.com/security.phtml?c=791 (date of reference: 20.01.2020).

[15] Shabalin A. M., Operating systems virtualization: opportunities and prospects of use in the training process, Human science: humanitarian research. 1 (27) 2017, pp.155-159. DOI: https://doi.org/10.17238/issn1998-5320.2017.27.155

[16] InfoWatch Traffic Monitor. User's manual, Infowatch , Moscow, 2017.