Approaches to Information Security in Educational Processes in the Context of Digitalization

Almaz Rafisovich Gapsalamov 1, Elvir Munirovich Akhmetshin 1, Rifat Rashatovich Sharipov 2, Vladimir Lvovich Vasilev 1, Tatyana Nikolaevna Bochkareva 1

1 Kazan Federal University, Elabuga Institute of KFU, 423604, Kazanskaya Street, 89, Elabuga, Russia
2 Kazan National Research Technical University named after A. N. Tupolev -KAI, 420111, K. Marx Street, 10, Kazan, Russia

Abstract – The article identifies the goals and objectives of digitalization in education, and presents the forms of implementation of educational processes. It investigates the methods of ensuring information security in educational institutions, and identifying 4 basic types of risk to build a threat model. Investigations into the invasion of our institution were carried out, vulnerabilities were identified for 4 types of risk, the results in the form of successful attacks were shown and recommendations for their elimination were developed. After the recommendations had been implemented, repeated testing was carried out. The results showed a significant decline in the number of successful attacks.

Keywords – digital economy, education, information, knowledge, information security.

1. Introduction

Modern digital network technologies open up entirely new possibilities for organizing economic life. In 2018, "the provision of accelerated implementation of digital technologies in the economy and social sphere" became one of the national development goals of the Russian Federation for the period until 2024.

DOI: 10.18421/TEM92-38
https://doi.org/10.18421/TEM92-38

Corresponding author: Elvir Munirovich Akhmetshin, Kazan Federal University, Elabuga Institute of KFU, 423604, Kazanskaya Street, 89, Elabuga, Russia.
Email: elvir@mail.ru

Received: 31 January 2020.
Revised: 03 May 2020.
Accepted: 12 May 2020.
Published: 27 May 2020.

© 2020 Elvir Munirovich Akhmetshin et al; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at www.temjournal.com

The May Decree of the President of the Russian Federation provides a definition for the national program "Digital Economy of the Russian Federation" [8]. The document sets goals for the program, in particular, "to increase domestic expenditures on the development of the digital economy from all sources (by the share in the country's gross domestic product) by at least three times compared to 2017". The assigned goal "to transform the priority sectors of the economy and social sphere, including healthcare, education, production, agriculture, construction, agriculture, transport and energy infrastructure, financial services, through the implementation of digital technologies and platform solutions" resulted in the development of several industry programs [4]. Therefore, all the concepts discussed above can be determined by the following characteristics [25].

1. Digitalization and integration of vertical and horizontal value chains. "Industry 4.0" provides for the digitalization and vertical integration of processes throughout the organization, from product development and procurement to production, logistics, and service. All data on operational processes, process efficiency, quality management and operational planning can be accessed online in the integrated network. It also uses augmented reality technologies, while the data is optimized for various platforms. The horizontal integration goes beyond internal operations and encompasses suppliers, consumers, and all key value chain partners. It uses multiple technologies: from tracking and control devices to integrated planning integrated with real-time execution [21].

2. Digitalization of products and services. Digitalization of products involves the addition of smart sensors or communication devices compatible with data analytics tools to the existing products, as well as the creation of new digital products designed to provide integrated solutions. The introduction of new methods of data collection and analysis allows companies to obtain data on the use of products and modify these products in accordance with the new requirements of end users [21].
3. Digital business models and customer access. The leading industry companies also expand their services with revolutionary digital solutions, including complex, personalized, data-driven services and integrated platforms. New digital business models often intend to obtain additional revenue from digital solutions, optimizing customer interaction and improving customer access. Digital goods and services are often designed to serve customers by providing them with end-to-end solutions in a separate digital ecosystem [21]. The availability of digital competencies is paramount to the successful implementation of the "Industry 4.0" concept. The strengthening of digital capabilities takes time and concentration of effort. In this context, it is important to move fast so as not to lose the "pioneer" advantages over competitors.

However, this process is inevitable, since any production seeks to increase efficiency and profitability, and the introduction of modern, automated, high-precision technology can significantly increase these indicators. This explains the necessity for standardization and unification in the field of industrial digitalization, which is reflected in the so-called "Industrial Internet of Things" (IIoT). The implementation of this technology provides equipping with measuring devices connected to a data exchange network for all the production equipment used by the enterprise; computerization of all workplaces; formation of a transmission system, automated processing and visualization of the collected data, integration of the equipment park and workplaces into a single information network [31].

The authors suggest schemes for organizing design and production procedures at industrial enterprises when performing full-scale tests with instrumentation products. They developed a block diagram of the algorithm for adjusting design, software and technical documentation in the product life cycle. The researchers define procedures that allow automating the development and subsequent maintenance of documentation for industrial enterprises to move toward working in a digital economy based on the principles of Industry 4.0. The article shows that the effect of introducing advanced technologies in the industry is achieved through the use of the Internet of Things and simulation technology with digital models of products as part of the developer's workplace. The results of this study can be used in the development of algorithms for computer-aided design of instrument-making (machine-building) digital production, operating in the digital economy of Industry 4.0 [33].

Therefore, the digitalization of world space is a modern requirement, an objective and unavoidable evolutionary direction in the development of civilization. Such circumstances inevitably lead to problems of state and individual security, as well as the manifestation of hidden and overt threats [9]. Their prevention and elimination require infrastructural security, psychological, resource, information and socio-economic preparedness, strategic readiness of the state system for crises, problems, and protests, creative activity of citizens, along with profoundly focused cooperation of all participants in the long-term development process [30].

The education area also undergoes a digital transformation of its activities. The educational institution experiences all of the above threats to information security due to the use of digital technologies [16]. Thus, the need for research on effective methods of information security at an educational institution is growing.

2. Literature Review

2.1. Digitalization in Education

Education is one of the first areas which started active work in this direction. Digitalization in education refers to the implementation of computer tools in education using digital educational resources [3].

The digital educational environment is an organically functioning set of information systems and their tools that provide the solution to numerous problems of the educational process at modern educational institutions. The digital educational environment uses various information systems, which for various reasons can be convenient, effective and promising in utilizing educational resources. Such specificity is anticipated by constant transformation dynamics and improvement of the environment related to the constant introduction of information technology innovation [27].

The development of the continuing education strategy in the context of its digitalization is examined in terms of the principle of systematic research regarding the indicated problem based on the understanding of the following factors:

1) the integrity of the continuing education system in all the diversity of its institutional and non-institutional components;
2) differentiation of the components of the continuing education system as elements, the properties and functions which are determined by their essence as part of the whole system;
3) system integrity through the system-forming concept of "communication";
4) the aggregate of relationships (the considered "forms") and their characteristics providing structural integrity and organization of the continuing education system [34].
In this regard, the main purpose of the digitalization process is to ensure a more effective return from all processes involved in digitalization by increasing the sphere of influence, involving participants in educational relations, expanding the range of educational services, etc. This determines the key objectives of digitalization in education [26]:

1. Implementation of digital technologies in the educational process, including interaction at all levels of the educational environment: managerial, informational, educational, etc.
2. Providing the collective use of digital resources and access to them in the "cloud" resources to all the participants in educational relations.
3. Training and continuous development in terms of advanced training of teachers within educational institutions on the use of digital technologies in educational activities; creation of digital educational resources, as well as communication and feedback within the digital educational environment.
4. Ensuring the motivation to improve the professionally-oriented use of digital technologies by teachers and learners.
5. Development and modeling innovative development conditions through the introduction of digital technologies in the educational process and the educational environment at an educational institution: for example, the terms of engagement between international partner universities, the creation of electronic professional portfolios, etc.
6. Providing information and consulting services on the use of digital and cloud technologies with unlimited resources.
7. Accumulation, systematization, and dissemination of information on the use of digital and cloud technologies in the digital educational environment within an educational institution.

Digitalization of education can be implemented in various forms [24]:

1. Partial or complete replacement of traditional paper media by creating an electronic environment (electronic libraries, textbooks, task books, video lectures, etc.), including its accessibility using various devices.
2. Creating distance (including online) learning. This will allow developing individual educational trajectories for students, creating an interactive electronic environment between the participants in the educational process.
3. The use of artificial intelligence technologies. Thus, in the next 5-10 years, it is planned to develop systems for the automatic translation of texts and speech from any language that will make it possible to easily perceive other people's speech [8]. This means that electronic resources, libraries of leading world universities and lectures of the best teachers will be available to all students, regardless the language they speak.
4. Implementation of project activities and game learning. The use of projects in the educational process allows students to realize their potential based on their abilities and preferences. Game activities will help them to acquire new knowledge and skills discreetly and unobtrusively. The use of games motivates students to continue the learning process.

Thus, the introduction of digitalization in education will allow changing or rethinking the existing educational process, as well as increasing its attractiveness.

2.2. The Current State of Information Security in Education

The integrated provision of information security at educational institutions should be standardized and controlled year-round, in real-time, around the clock. At the same time, the security system has to consider the entire life cycle of information, from the moment of its appearance to its complete destruction or loss of significance for the organization [1]. [19]. The analysis of several papers [2], [28], [22], brings up the possibility of defining common objectives for information security in educational institutions:

1. Prevention of leakage, theft, loss, distortion, and falsification of information due to its replicability [12];
2. Prevention of threats to the security of an individual, enterprise, society, and state due to disclosure or distortion of information [12];
3. Prevention of unauthorized actions to destroy, modify, distort, copy, or block information, which may lead to a decrease in its potential effectiveness [14];
4. Prevention of various types of unlawful interference in information resources and enterprise systems [12];
5. Provision of the legal protection for information as an object of ownership (exclusion of the possibility of its illegal replication) [12];
6. Protection of constitutional rights regarding citizens to maintain personal secrets and confidentiality of personal data stored in enterprise information systems [12];
7. Confidentiality of documented information in accordance with the legislation (the rights of secrecy, access, and distribution, etc.) [12].

There are numerous solutions and approaches to achieve these goals. Yet, some basic measures are especially critical and important for educational institutions. Those involve [15]:

1) Control of access to both workplace information and application programs.
2) The need to grant access only to authorized users who would subsequently have access to information and applications [19];
3) Development of authorization procedures that determine which users can have access to certain applications and information, and provide appropriate measures to introduce such procedures into the organization [19];
4) Development of procedures to restrict access to files: to use external and internal labels to indicate the type of information contained in files and the required level of security; to restrict access to the premises in which the archives, files, and data libraries are stored; to use organizational measures and firmware to restrict access to files to authorized users;
5) Protection of data integrity, error checking, provision of its completeness and accuracy. The accuracy of information has to be verified using procedures to compare the obtained processing results with the expected ones [19];
6) Protection of system software. When developing programs, protection measures should involve procedures to make changes of the program, its acceptance and user-testing prior to implementation [19];
7) Cryptographic closure when transferring information over insecure communication lines (Internet), where it can be easily intercepted by an attacker.

3. Methodology

To build a model of information security threats, the authors analyzed various methods and approaches associated with information security risks at educational institutions [14], [32].

The study [29] identifies several major information security risks in the field of education under digitalization. However, in this study, the authors decided to highlight the most significant risks for the institution under consideration. The Elabuga Institute of Kazan Federal University (EIKFU) was selected as the object of study. The researcher I.V. Anikin [1], [2] believes that the implemented attacks result from vulnerabilities in software products, network services or insufficient information security measures. This factor was examined as APT (advanced persistent threat), which is a high precision cyberattack that allows stealing confidential data in information systems and networks. When testing the system, the authors simulated attacks from an external network and registered implemented attacks. In doing this, the authors did not have any advance information about the system – they used the "black box" method.

Other significant risks were directly related to the active employees of the EIKFU. The ideal network protection from attacks does not guarantee the full confidence of security due to the large numbers of employees participating in information interaction. They can be potential violators of information security both intentionally and not intentionally. For instance, they can unintentionally click an incorrect link or transfer their credentials to the attackers. These methods involve phishing, which is a type of Internet fraud, built on the principles of gaining access to critical data, accounts, etc. When testing the users, the authors sent them email messages comprising various advertising or working nature with inserted links to make them click the link redirecting them to a third-party site with malicious code.

Another important risk associated with employees is ransomware, which is malicious software that contains a message and images provoking an employee to start malicious processes at his or her automated workplace (AWP). Similarly to phishing testing, the authors sent various e-mail messages to employees to make them click on a pre-arranged link with malicious software, and they also sent veiled executable files with a hidden "exe" extension or js scripts veiled under the doc. or other office applications.

When testing users for phishing and ransomware, the authors used their corporate mailboxes, where fraudulent messages were sent. When the attack turned out to be successful, and the user clicked on the link or launched malware, the administrator received a message with the IP address of the attacked workplace and the type of successful attack. This allowed collecting statistics on all the attacks.

In addition to all of the above, the researchers considered another important factor – the distribution of BYOD (Bring Your Own Device), which allows users to store corporate data locally on their mobile devices. This fact leads to additional information security risks. When using BYOD, the employees cannot always provide adequate protection for their personal devices from leakage of confidential information. At the same time, the administration cannot prohibit them from using mobile devices, due to the necessary mobility of employees in the performance of their duties [10]. The researchers
tested these employees when they are remotely connected to the corporate system, identified their connection methods, and examined the vulnerabilities of their devices.

4. Results

We can consider the effectiveness of approaches to information security of educational processes in the context of digitalization.

The authors conducted a study of the corporate education system, which included computer facilities, network interactions, and gateways to the global Internet. The automated workplaces (AWPs) were equipped with software working in the education system and had online access services to various network infrastructures (such as access to online bibliographic systems, etc.).

To imitate the real scenario in which an intruder attacks the network, the researchers decided to conduct a penetration test using the "black box" method – when the intruder does not have any advance information about the system.

Based on vulnerability studies of such systems [18] the authors chose the following attack directions:

- Network attack;
- Attack on the employees’ e-mails;
- Use of social engineering techniques.

The testing allowed selecting the following popular tools: Nmap, Metasploit, eMailTrackerPro, Ophcrack, etc. The researchers also called the employees to obtain confidential and personal information, presenting themselves as security officers of the selected educational institution.

The testing results are presented in Figure 1.

Figure 1 shows that phishing attacks were implemented in 77% of cases; APT threats – in 47% of cases. Fraudulent actions turned out successful in 35% of cases; data interception with BYOD – in 27% of cases.

The testing results allowed developing recommendations to reduce the risk of security threats. Those include:

1. Anti-phishing recommendations [20]:
   - when receiving suspicious links, one should make sure that the sender exists as a real person to be trusted;
   - one must not enter the websites that require entering personal data by the link; it is better to type the address manually (the login procedure has to be performed through reliable devices and networks);
   - it is recommended to use and regularly update anti-virus products, especially if they offer anti-phishing solutions (for example, in the form of the anti-phishing module).

2. Recommendations on protection against APT attacks [7]:
   - it is recommended to apply intelligent methods for detecting anomalies in a computer system, including expert analysis of the network traffic, diagnostics of social engineering techniques by users specially trained for this purpose, etc.;
   - one has to use standard signature methods, although they may not be effective enough due to the narrow focus of attacks and the unique nature of Instrumentalities used for committing cybercrimes.

3. Anti-fraudulent recommendations [5]:
   - one must not click on the screen button with the inscription type "Click on me", "Next", "Get your bonus", etc.;
   - if possible, it is recommended to immediately close the software and inform the information security service.

4. Recommendations for using BYOD devices [13]:
   - one has to ensure the secure, authorized access to data;
   - it is recommended to install antivirus software;
   - when connecting to the institution, one has to use only secure VPN (Virtual Private Network) tunnels.

To assess the effectiveness of the above countermeasures aimed at eliminating the identified threats, the infrastructure of the educational institution was re-examined after the improvements were made. The results are shown in Figure 2.
Figure 2 shows a noticeable decrease in the number of realized attacks, which can be attributed to the effectiveness of countermeasures. However, protection from social engineering methods remains the major insufficiently resolved problem, since in this case the attacks are directed not at the technical system elements, but directly at a certain user. Of these, phishing attacks and the use of personal information processing devices remain of most concern.

5. Discussion

In this study, the authors examined various approaches to ensuring information security at educational institutions under modern digitalization. Some of them are discussed below – those selected for the analysis. The study by Razuvaeva et al. [23] substantiates the relevance of information security in digitalization but does not provide any methods or approaches. The work by Kulikova et al. [17] justifies the relevance of digitalization in the Russian Federation and considers the security approach at the state level. In addition, Bürger et al. [6] systematize approaches to information security, describing various methods and tools, but do not present any specific studies.

The works by Anikin [2], Sharipov et al. [28], Raikhlin et al. [22] describe measures to ensure information security at educational institutions. Indeed, the proposed measures seem effective and yield results, but these are mainly organizational-type measures. In real life, one faces specific actions that require specific countermeasures.

Certain solutions and approaches to information security are examined in the works by Katasev [15], Gibadullin [11]. Those are very significant, crucial and effective, However, not all of them are appropriate in specific cases. Considering the applicability of information security methods, one should always focus on the object of application, in this study – the educational institutions. This is the first study to systematize the most significant risks and test them at a specific educational institution. The authors identified criteria such as phishing, APT attacks, fraudulent software and the use of BYOD. The results of the study were a decrease in the initially detected phishing attacks by 81.8%, APT attacks – by 95.7%, attacks due to fraudulent software – by 88.6%, and attacks using BYOD – by 74%. The authors believe this approach to be effective, although it is impossible to eliminate all possible attacks since there is a constant emergence of new approaches and attack technologies. Their timely identification allows reconfiguring the security system.

6. Conclusions and Recommendations

The results of this study allow formulating the following conclusions and recommendations:

1. The authors analyzed current trends in the development of digital technologies and their impact on the activity of the institution employees. They defined the key characteristics in considering the concept of digitalization for different state areas.

2. The study revealed the major factors determining the education system in the context of digitalization, as well as the main objectives of education digitalization.

3. The researchers have identified characteristics of the educational process under digitalization given the increasing threats to information security. They examined the most common methods of attacking an educational institution’s information security system.

4. The paper reviews the problems of information security in the modern economy, considering the increasing role and relevance of digital technologies.

5. The authors evaluated the most common methods of attacking an information security system at the selected educational institution. They selected 4 criteria to assess the current state of information security on the results of penetration tests, various types of attacks and attacks using social engineering methods.

6. The test results allowed forming recommendations to eliminate the vulnerabilities of the chosen educational institution, which were subsequently implemented to improve the security system. Repeated testing of the protected system showed a decrease in the number of realized attacks.
The approaches to information security developed by the authors are crucial in educational processes, especially in the context of digitalization. They allow identifying potential vulnerabilities and apply preventive measures even at the initial stages of any educational system, to avoid the possibility of known attacks. The detection of attacks related to the companies' employees was an important feature of this study, as the largest number of attacks fall precisely on the actions of employees.

7. Conclusion

In this paper, the authors presented approaches that allowed them to significantly reduce the influence of threats to information security using the example of selected educational institution. However, in addition to the countermeasures described above, one also has to implement recommendations for protecting networks, network interfaces, and network resources. It is necessary to conduct periodic training for employees of an educational institution for the protection of information. The authors also suggest periodic infrastructure testing to identify new vulnerabilities in order to prevent them. The recommended measures allowed reducing threats to information security at the selected educational institution and thereby increasing the reliability of information systems under digitalization.

Acknowledgements

The reported study was funded by Russian Foundation for Basic Research (RFBR), project "Digitalization of the economy: the creation of a protectionist model of Russian education" number 19-29-07037. Period of the project: 2019-2022.

References


