

Journal Scientific and Applied Research, Vol. 30, 2026
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

INFORMATION SECURITY IN HIGHER EDUCATION ADMINISTRATION: ANALYSIS OF RISKS AND EMPLOYEE ATTITUDES

Donika V. Dimanova[1], Eda E. Zakir[2]

[1]Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: d.dimanova@shu.bg
[2]Department of Communication and Computer Engineering and Security Technologies, Faculty of Technical Sciences, Konstantin Preslavsky University of Shumen, Shumen 9712, 115 Universitetska St., e-mail: e.zakir@shu.bg

Abstract: *The digitalization of administrative and academic processes in higher education institutions increases their dependence on information systems while simultaneously creating new risks to the security of processed information. The paper analyzes the main information security risks in university administration and presents the results of a survey conducted among employees of a higher education institution. Particular attention is given to the human factor, the protection practices applied, perceived cyber risks, and the need for additional organizational and technical measures. Based on the results obtained, guidelines are formulated for enhancing information security and developing a stronger security culture within the university environment.*

Key words: *Information security, Higher education institution, Cyber risks, Human factor, Information systems, Training.*

1. Introduction

The development of information technologies and the accelerated digitalization of administrative processes have made information security an essential factor for the sustainable functioning of modern organizations. Higher education institutions are particularly dependent on the reliability of information systems, as they process significant amounts of personal, academic, personnel, financial, and official data on a daily basis [2, 6].

Information security encompasses a set of organizational, technical, and managerial measures aimed at ensuring the confidentiality, integrity, and availability of information. The effectiveness of protection does not depend solely on the availability of technical safeguards, but also on the interaction between technologies, processes, and the human factor [2]. This interdependence is especially important in the university environment, where information resources are used by a wide range of users with different functions, access rights, and levels of training.

The expanding use of university information systems, email, document management systems, cloud services, and collaborative platforms improves administrative efficiency, but at the same time increases the number of potential points at which security incidents may occur. The main risks include unauthorized access, loss or disclosure of data, phishing attacks, malware, improper management of user access rights, and human error [3, 4, 6].

The human factor is of particular importance. Despite advances in technical protection measures, the use of weak passwords, insufficient awareness, incorrect transmission of documents, and susceptibility to social engineering may compromise even well-protected information systems [3]. Therefore, training and the development of a sustainable information security culture should be regarded as an integral part of the overall protection system rather than as an additional activity.

The aim of the present paper is to analyze the main information security risks in the administration of a higher education institution and, through the results of a survey, to identify employees' attitudes and practices regarding the protection of information resources.

To achieve this aim, the paper applies analysis of specialized sources, systematization of the main risk factors, and quantitative and qualitative analysis of the results of the conducted survey.

2. Exposition

Main Information Security Risks in University Administration

The information environment of a higher education institution is characterized by intensive data exchange among administrative units, academic staff, students, and external institutions. These processes involve the handling of personal data, academic records, personnel information, financial documents, and official correspondence, which requires a systematic approach to information security management [2, 5, 6].

The main risks can be classified into three interrelated groups: human, technological, and organizational.

Human-related risks are associated with user actions or omissions that may lead to the compromise of information. Typical examples include the use of weak or reused passwords, sharing user accounts, incorrectly addressing email messages, and insufficient ability to recognize phishing and other forms of social engineering [3].

Technological risks arise from the dependence of administrative processes on information systems and communication infrastructure. They include software vulnerabilities, system outages, compromised user accounts, ransomware, malware, and insufficiently reliable authentication mechanisms [4, 6].

Organizational risks are associated with the absence or inadequate implementation of internal policies, procedures, and risk management mechanisms. The formal existence of regulatory documents does not guarantee effective protection if risk management is not genuinely integrated into decision-making processes and everyday administrative practice.

The three groups of risks do not operate in isolation. A technological vulnerability may be exploited through human error, while an organizational weakness may increase the consequences of a technical incident. Therefore, effective information security management requires a comprehensive approach combining technological protection, clear organizational rules, and systematic user training [2, 3, 7].

Survey Methodology

To assess the state of information security and the protection of information flows in the administration of a higher education institution, an anonymous survey was conducted among employees from different structural units of the university. The aim was to determine employees' level of awareness of information security issues, the protection practices they apply, the risks they perceive, and the need for additional organizational and technical measures.

The survey was conducted in accordance with the principles of voluntary participation and anonymity. A total of 37 employees representing different structural units of the higher education institution took part. The questionnaire consisted of 20 questions grouped into four main thematic areas: general information about the participants, use of university information systems, information security and cyber risks, and assessment of the level of security and the need for additional measures.

The first group of questions focused on the participants' professional profile and the frequency of their use of university information systems. The second addressed the use of email, electronic administrative documents, cloud services, and personal devices. The third group examined practices related to passwords, two-factor authentication (2FA), recognition of phishing attacks, and behavior when receiving suspicious messages. The final part of the questionnaire focused on the assessment of information security and the preferred measures for its improvement.

The results were processed using quantitative and qualitative analysis. The quantitative component was based on the distribution of responses to the individual questions, while the qualitative analysis focused on interpreting the main trends, risk areas, and preferred measures for improving information security.

Results and Analysis

A total of 37 employees from different structural units of the higher education institution participated in the survey. The largest group consisted of representatives of academic departments - 10 respondents (27.0%), followed by participants who selected the category "Other" - 8 respondents (21.6%). Six respondents (16.2%) were from the IT department, while the administration and the library were represented by 5 respondents each (13.5%). The smallest group consisted of employees from dean's offices - 3 respondents (8.1%). This distribution ensured the participation of employees with different functions and varying levels of involvement in the processing and exchange of information.

The results indicate a high level of use of university information systems. Twenty-one respondents (56.8%) use them daily, 4 respondents (10.8%) use them several times a week, and 12 respondents (32.4%) use them less frequently. None of the participants indicated that they almost never use such systems. This confirms the significant dependence of administrative and academic processes on electronic data processing and information exchange.

From an information security perspective, this dependence increases the importance of reliable user identification, access control, protection of electronic communications, and regular staff training. The more intensively information systems are used, the greater the risk of compromised user accounts, unauthorized access, data loss, or human error.

Particularly indicative are the results concerning the risks perceived by employees (Figure 1).

The most serious threats identified were personal data leakage and the lack of information security training, each indicated by 23 respondents (62.2%). These were followed by the use of weak passwords and the spread of malware and computer viruses, each selected

by 22 respondents (59.5%). Phishing attacks were identified as a significant risk by 19 respondents (51.4%), while unauthorized access to information systems was indicated by 17 respondents (45.9%). A smaller proportion of respondents identified insufficient technical protection - 9 respondents (24.3%) - and the use of personal devices for access - 8 respondents (21.6%).

The data obtained indicate that a significant proportion of the perceived risks are directly or indirectly related to the human factor. Insufficient training, the use of weak passwords, and susceptibility to phishing attacks may increase the likelihood of security incidents even when technical protection measures are in place.

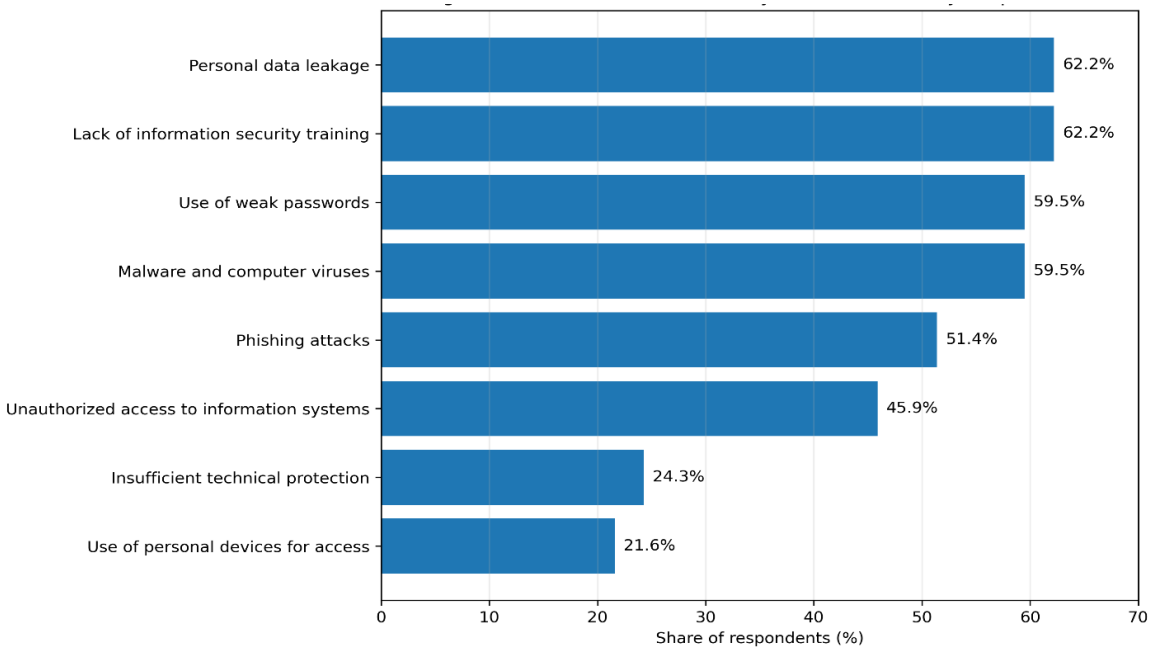


Fig. 1. Main Information Security Risks Identified by Respondents

This confirms the need for information resource protection to include not only technological solutions, but also systematic measures aimed at improving users' knowledge and sense of responsibility [3].

The responses concerning the preferred measures for improving information security also provide important insights (Figure 2). A total of 26 respondents (70.3%) indicated the need for cybersecurity training, representing the highest reported share. The use of stronger passwords was supported by 20 respondents (54.1%), two-factor authentication by 18 respondents (48.6%), and regular software updates by 16 respondents (43,2%).

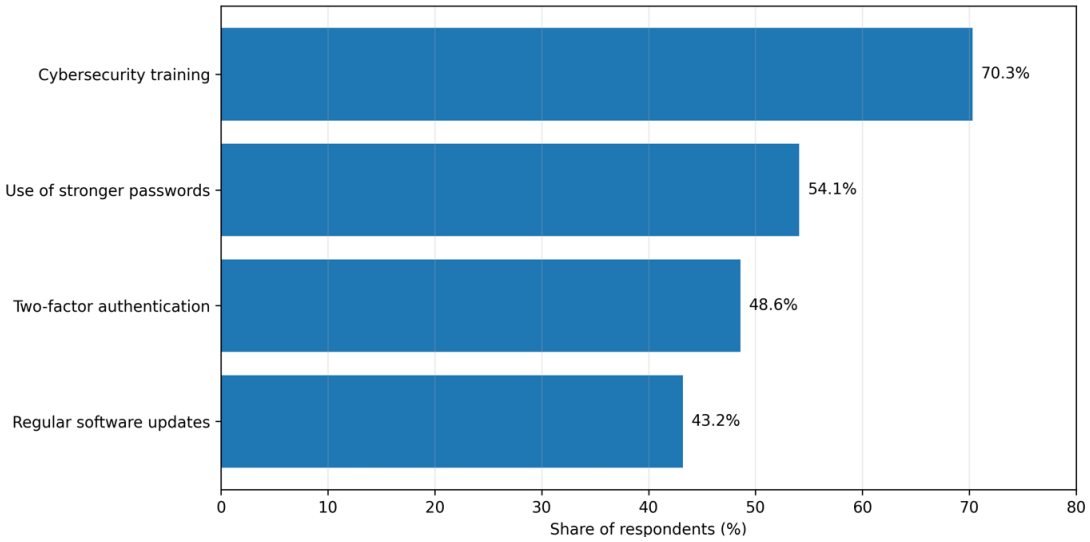


Fig. 2. Measures Proposed by Respondents to Improve Information Security

These results indicate a clear preference for a combined approach in which staff training is complemented by technical protection measures. It is particularly noteworthy that training received greater support than any individual technological solution. This suggests that employees perceive information security not only as a technical issue, but also as an organizational and behavioral one.

In summary, the results indicate a relatively good level of awareness of the main threats, while at the same time revealing a clear need for additional training and wider implementation of technical protection mechanisms. The human factor emerges as a central element both in the occurrence of risks and in their mitigation, which should be taken into account when developing future information security policies in higher education institutions.

Guidelines for Enhancing Information Security

The results of the survey indicate that improving information security in a higher education institution should be based on a comprehensive approach combining organizational, technical, and training measures. Of particular importance is the fact that the largest share of respondents identified cybersecurity training as necessary, confirming the role of the human factor as a key element in the overall protection system.

First, a systematic policy for staff training and awareness should be developed. It should include the recognition of phishing attacks, safe use of email, handling of sensitive information, password management, and appropriate responses to suspicious events. Such training should not be conducted as a one-time activity, but rather on a regular basis and in accordance with the evolving cyber threat environment [3, 4, 7]. In addition, the development of digital competencies should not be limited to currently used information systems but should also prepare users for the critical and secure adoption of emerging digital technologies [8].

A second area concerns the improvement of user account and access management. The use of strong and unique passwords, multi-factor authentication (MFA), and clearly defined user roles can significantly reduce the risk of unauthorized access and compromised user accounts [2, 6]. The importance of these measures is also confirmed by the survey, in which 54.1% of respondents supported the use of stronger passwords and 48.6% supported two-factor authentication.

A consistent policy for updating operating systems, applications, and information services should also be maintained. Timely installation of security updates reduces the possibility of known vulnerabilities being exploited in cyberattacks and should form part of the centralized management of university information infrastructure [1, 4]. In the survey, 43.2% of respondents identified regular software updates as a necessary measure for improving security.

Internal policies and procedures for handling information are also of substantial importance. They should regulate the granting, modification, and termination of access rights, the handling of electronic documents, data backup and recovery, as well as procedures for reporting and analyzing security incidents. Clear allocation of responsibilities and classification of information according to its sensitivity provide a more reliable organizational basis for protecting information resources [7].

Another important area is strengthening the resilience of the information infrastructure through reliable backup and recovery mechanisms. Maintaining up-to-date backup copies and periodically testing recovery procedures are particularly important in incidents involving ransomware, technical failures, or human error [1, 6].

In summary, improving information security in a higher education institution should be regarded as a continuous process rather than as the one-time implementation of individual technical solutions. The greatest effectiveness can be achieved through a combination of training, access control, reliable authentication, system updates, clear internal rules, and resilient backup and recovery mechanisms. This combination makes it possible both to mitigate technological risks and to reduce dependence on human error.

3. Conclusion

Information security in higher education institutions is directly linked to the reliable functioning of administrative and academic processes. The growing dependence on information systems, electronic communications, and digital services increases the need for systematic risk management and the implementation of complementary organizational and technical measures.

The results of the survey show that employees recognize the main information security risks, placing particular emphasis on personal data leakage, insufficient training, weak passwords, malware, and unauthorized access. At the same time, there is a clear need for regular cybersecurity training and wider implementation of modern protection mechanisms.

Enhancing information security should be based on an integrated approach combining the development of staff competencies, effective access control, reliable authentication, regular system updates, clear internal rules, and resilient backup and recovery mechanisms. Such an approach provides a basis for more reliable protection of information resources and for the sustainable operation of the university information environment.

References

[1] Atanasova-Mollova, D. K. Risks and Threats to Information Protection from Artificial Intelligence. In: Bulletin of the Faculty of Police, No. 18/2025, Academy of the Ministry of Interior, 2025, pp. 103-113.

[2] Dimov, P., Zdravkov, Z., Dobreva, H. Information Security. G. S. Rakovski National Defence College, Sofia, 2021.

[3] Domozetov, H. Human Factor and Information Security. In: Information & Security: An International Journal, 1998, No. 1, pp. 46-60.

[4] Draganov, I. Cybersecurity in the Education Sector: Importance, Threats and Future. Skill Catalyst, 2 July 2024.
[5] Personal Data Protection Act. Promulgated, State Gazette, No. 1 of 4 January 2002; amended, State Gazette, No. 69 of 31 July 2026.
[6] Stoitsov, G. Information and Communication Security. Paisii Hilendarski University of Plovdiv, Plovdiv, 2020.
[7] Vasilev, D. Information Security Management in Educational Institutions: Policies, Procedures and Good Practices. In: Information and Communication Technologies in Business and Education: Proceedings of the International Scientific Conference on the Occasion of the 55th Anniversary of the Department of Informatics at the University of Economics – Varna. Varna: Science and Economics Publishing House, 2024, pp. 213-219. ISBN 978-954-21-1184-9.
[8] Tasinov, T. Y., Toncheva, S. K. Anticipatory Technological Preparation and Digital Health Competencies in Nursing and Midwifery Education. Proceedings of the XIX National Forum of Health Care Specialists and Poster Session for Students “Fair Access to Quality Health Care”, Shumen, 24–25 October 2025, pp. 97–103. [Online]. Available: https://journals.mu-varna.bg/index.php/conf/issue/view/693.