
**September 22-23, 2022. Budapest, Hungary, pp.106-111, pages 106–111**

# The Holistic Approach to Cybersecurity in Academia

**Arina Alexei, Pavel Nistiriuc, Anatolie Alexei**

https://doi.org/10.1145/3551504.3551516

## Abstract

Academic institutions are increasingly implementing digital services and new technologies, for a modern and accessible educational environment. But the virtual environment creates unknown vulnerabilities that need to be addressed properly. The holistic approach to cybersecurity in academia as a system has major benefits. But the main question is how this can be done in practice, as long as universities are heterogeneous complex environments. The proposed solution can be used to implement a security system in academia, is compliant with the security standard ISO 27001 and developed by applying the scientific method of Security Requirement Engineering.

*Keywords: cybersecurity, virtual environment vulnerability, security systems*

## References

1. Xin Huang, Paul Craig, Hangyu Lin, and Zheng Yan. 2016. SecIoT: a security framework for the Internet of Things. In Security and Communication Networks, vol. 9, no. 16, pp. 3083–3094. https://dl.acm.org/doi/10.1002/sec.1259
2. Arina Alexei, and Anatolie Alexei. 2021. Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance. In International Journal of Scientific & Technology Research, vol. 10, no. 3, pp. 128–133.
3. Julian Jang-Jaccard, and Surya Nepal. 2014. A survey of emerging threats in cybersecurity. In Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973–993. DOI: 10.1016/j.jcss.2014.02.005.
4. Arina Alexei. 2021. Ensuring information security in public organizations in the Republic of Moldova through the ISO 27001 standard. In Journal of Social Sciences, vol. IV(1). DOI: 10.52326/jss.utm.2021.4(1).11


**September 22-23, 2022. Budapest, Hungary, pp.106-111, pages 106–111**

5. Arina Alexei, and Anatolie Alexei. 2021. Cyber Security Threat Analysis In Higher Education Institutions As A Result Of Distance Learning. In International Journal of Scientific & Technology Research, vol. 10, no. 3.
6. Manal M. Yunis, and Kai S. Koong. 2015. Conceptual Model for the Development of a National Cybersecurity Index: An Integrated Framework. In AMCIS.
7. Alessandro Oltramari, Noam Ben-Asher, Lorrie Cranor, Lujo Bauer, and Nicolas Christin. 2014. General Requirements of a Hybrid-Modeling Framework for Cyber Security. In 2014 IEEE Military Communications Conference, pp. 129-135. DOI: 10.1109/MILCOM.2014.28
8. Arina Alexei. 2022. Design & development of a cyber security conceptual framework for higher education institutions in the Republic of Moldova. In Scientific and Practical Cyber Security Journal (SPCSJ), vol. 6, no. 1, pp. 35–52.
9. Huma Rehman, Ashraf Masood, and Ahmad Raza Cheema. 2013. Information Security Management in academic institutes of Pakistan. In 2013 2nd National Conference on Information Assurance (NCIA). DOI: 10.1109/NCIA.2013.6725323
10. Noran Shafik Fouad. 2021. Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. In Journal of Cyber Policy, vol. 6, no. 2, pp. 137–154. DOI: 10.1080/23738871.2021.1973526
11. Biswajit Panja, Dennis Fattaleh, Mark Mercado, Adam Robinson, Priyanka Meharia. 2013. Cybersecurity in banking and financial sector: Security analysis of a mobile banking application. In 2013 International Conference on Collaboration Technologies and Systems (CTS), pp. 397–403. DOI: 10.1109/CTS.2013.6567261
12. Lynne Coventry, and Dawn Branley. 2018. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. In Maturitas, vol. 113, pp. 48–52. DOI: 10.1016/j.maturitas.2018.04.008
13. Uchenna Daniel Ani, Hongmei He, and Ashutosh Tiwari. 2019. Human factor security: evaluating the cybersecurity capacity of the industrial workforce. In Journal of Systems and Information Technology, vol. 21, no. 1, pp. 2–35. DOI: 10.1108/JSIT-02-2018-0028
14. Robert Müller-Török, and Alexander Prosser. 2021. Teaching requirements of a digitised public administration. In Pro Publico Bono - Magyar Közigazgatás, vol. 9, no. 1, pp. 2–15. DOI: 10.32575/ppb.2021.1.1
15. Arina Alexei. 2021. Network security threats to higher education institutions. In CEE e|Dem and e|Gov Days, pp. 323–333. DOI: 10.24989/ocg.v341.24
16. Ross Brewer 2016. Ransomware attacks: detection, prevention and cure. In Network Security, vol. 2016, no. 9. DOI: 10.1016/S1353-4858(16)30086-1
17. Juan Fernando Balarezo, Song Wang, Karina Gomez Chavez, Akram Al-Hourani, and Sithamparanathan Kandeepan. 2022. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. In Engineering Science and Technology, an International Journal, vol. 31, p. 101065. DOI: 10.1016/J.JESTCH.2021.09.011
18. Edyta Karolina Szczepaniuk, Hubert Szczepaniuk, Tomasz Rokicki, and Bogdan Klepacki. 2020. Information security assessment in public administration. In Computers and Security, vol. 90, p. 101709. DOI: 10.1016/j.cose.2019.101709
19. Robert I. MacCuspie, Harvey Hyman, Chris Yakymyshyn, Sesha S.Srinivasan, Jaspreet Dhau, and Christina Drake. 2014. A framework for identifying performance targets for sustainable nanomaterials. In Sustainable Materials and Technologies, vol. 1–2, pp. 17–25. DOI: 10.1016/J.SUSMAT.2014.11.003

20. Bichanga Walter Okibo, and Obara Brigit Ochiche. 2014. Challenges Facing Information Systems Security Management in Higher Learning Institutions: A Case Study of the Catholic University of Eastern Africa – Kenya. In International Journal of Management Excellence, vol. 3, no. 1, pp. 336–349. DOI: 10.17722/ijme.v3i1.122
21. Ivano Bongiovanni. 2019. The least secure places in the universe? A systematic literature review on information security management in higher education. DOI: 10.1016/j.cose.2019.07.003In Computers and Security, vol. 86, pp. 350–357. DOI: 10.1016/j.cose.2019.07.003
22. Jorge Merchan-Lima, Fabian Astudillo-Salinas, Luis Tello-Oquendo, Franklin Sanchez, Gabriel Lopez-Fonseca and Dorys Quiroz. 2020. Information security management frameworks and strategies in higher education institutions: a systematic review. In Annals of Telecommunications. DOI: 10.1007/s12243-020-00783-2
23. Neil Francis Doherty, Leonidas Anastasakis, and Heather Fulford. 2011. Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. In International Journal of Information Management, vol. 31, no. 3, pp. 201–209. DOI: 10.1016/j.ijinfomgt.2010.06.001
24. Alin-Ciprian Cojocariu, Ion Verzea, and Rachid Chaib. 2020. Aspects of Cyber-Security in Higher Education Institutions. In Innovation in Sustainable Management and Entrepreneurship, pp. 3–11. DOI: 10.1007/978-3-030-44711-3_1
25. Council of the European Union and European Parliament. 2016. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Retrieved February 28, 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148)
26. ISO/IEC 27001: Information Security Management. International Organization for Standardization," Geneva, Switzerland, 2013. Retrieved December 02, 2021 from https://www.iso.org/isoiec-27001-information-security.html
27. George Disterer. 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. In Journal of Information Security, vol. 04, no. 02. DOI: 10.4236/jis.2013.42011
28. Abbass Asosheh, Parvaneh Hajinazari, and Hourieh Khodkari. 2013. A practical implementation of ISMS. In 7th International Conference on e-Commerce in Developing Countries: with focus on e-Security, 2013, pp. 1-17. DOI: 10.1109/ECDC.2013.6556730
29. Veliko Ivanov, Monika Tzaneva, Alexandra Murdjeva, and Valentin Kisimov. 2011. Securing the Core University Business Processes. In Camenisch, J., Kisimov, V., Dubovitskaya, M. (eds) Open Research Problems in Network Security. iNetSec 2010. Lecture Notes in Computer Science, vol 6555. Springer, Berlin, Heidelberg. DOI: 10.1007/978-3-642-19228-9_9
30. Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. 2006. Applying a Security Requirements Engineering Process. In Gollmann, D., Meier, J., Sabelfeld, A. (eds) Computer Security – ESORICS 2006. ESORICS 2006. Lecture Notes in Computer Science, vol 4189. Springer, Berlin, Heidelberg. DOI: 10.1007/11863908_13
31. Kristian Beckers, Stephan Fabbender, Maritta Heisel, and Holger Schmidt. 2012. Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation. In 2012 Seventh International


**September 22-23, 2022. Budapest, Hungary, pp.106-111, pages 106–111**

Conference on Availability, Reliability and Security, pp. 242–248. DOI: 10.1109/ARES.2012.35

32. Shafiq Ur Rehman, and Volker Gruhn. 2018. An Effective Security Requirements Engineering Framework for Cyber-Physical Systems. In Technologies (Basel), vol. 6, no. 3, p. 65. DOI: 10.3390/technologies6030065
33. Shafiq Ur Rehman, Christopher Allgaier, and Volker Gruhn. 2018. Security Requirements Engineering: A Framework for Cyber-Physical Systems. In 2018 International Conference on Frontiers of Information Technology (FIT), pp. 315-320. DOI: 10.1109/FIT.2018.00062