

DOCTORAL (PHD) STUDIES COURSE UNIT DESCRIPTION

Course unit title	Scientific areas	Faculty	Institute, department
Cybersecurity of Systems	Informatics (N009)	Faculty of Mathematics & Informatics	Institute of Computer Science, Cybersecurity laboratory

Study method	Number of credits ECTS	Study method	Number of credits ECTS
lectures	1 (autumn)	consultations	1
individual	4	seminars	1

Summary
This course introduces the fundamental concepts of cybersecurity (CS), enabling students to delve into more complex topics, including horizontal CS applications in computer science. The course covers the entire spectrum of secure digital space management, the modeling of digital twins relevant to the field, the security of information and network communication flows, and digital investigations. CS is inseparable from organizational maturity, best practices, and the human dimension as both the creator and user of digital systems. Thus, the topics will range from compliance with system requirements and applicable standards to risks posed by human factors, taking into account the latest scientific achievements and trends in technology applications. The course examines various risk mitigation strategies designed to reduce the impact of vulnerabilities, neutralize threats, and protect an organization's data and system resources. The aim of this course is to provide doctoral students with knowledge of cybersecurity and to develop their ability to formulate security requirements for software, including doctoral prototypes, identify the attack surface of computer systems, and assess threats and risks using appropriate algorithmic and technological solutions and methodologies. Main course topics: • A holistic approach to cybersecurity • Security policies, standards, and EU directives • Attack surface identification, threat and risk assessment • Software security assessment methods and standards • Vulnerability detection methods • Digital twin modeling • Digital forensics methods • Malicious code analysis environments and behavioral analysis • Application of modern technologies in defense • Security of the research <i>Practical assignment:</i> Based on the topic of your research, select a cybersecurity project to implement, model the attack surface, utilize the cybersecurity testing ground to test cybersecurity defense tactics,

conduct experiments to manage cybersecurity threats and evaluate the selected tactics, prepare a project report, and present it in a presentation.

Main literature

Cornish, P. (Ed.). (2021). The Oxford Handbook of Cyber Security. Oxford University Press.
<https://doi.org/10.1093/oxfordhb/9780198800682.001.0001>

Stevens, T. (2026). Cyber Risk. Bristol University Press. <https://doi.org/10.51952/9781529256048>

Velu, V. K. (2022). *Mastering Kali Linux for advanced penetration testing : become a cybersecurity ethical hacking expert using metasploit, nmap, wireshark, and burp suite* (Fourth edition.). Packt Publishing, Limited. <https://doi.org/10.0000/9781801812672>

Lecturer(s) (name, surname)	Science degree	Main publications
Prof. Linas Bukauskas	dr.	https://elaba.mb.vu.lt/mif/?aut=Linas+Bukauskas
Assoc. prof. Agnė Brilingaitė	dr.	https://elaba.mb.vu.lt/mif/?aut=Agnė+Brilingaitė