Funded by the European Union

CYBERCHALLENGE Challenges Solving in Cybersecurity Study Program

CYBERCHALLENGE *- Challenges Solving in Cybersecurity Study Program No. 2024-1-LT01-KA220-HED-000252504*

Newsletter

August 2025

About Cybersecurity curriculum

The increasing prevalence of cyber threats and the growing reliance on digital technologies make it imperative to implement a robust cybersecurity curriculum. Cooperation between universities is a great opportunity to improve the quality of education, create innovative study programs, and enrich the student experience. To achieve the best results, it is important to choose the right methodologies and strategies. We will use hMOOCs, Federated Education and Challenge-based learning methodologies to implement the Cybersecurity digital curriculum. The proposed Cybersecurity curriculum intends to familiarize learners with key subjects: Fundamentals of Cybersecurity, Identity and Access Management, Cyberattacks and Cyber Defenses and Cyber Security Management. Brief description of the associated courses and contextualize them in Cybersecurity scenarios:

Fundamentals of Cybersecurity

Cybersecurity is a complex field that involves a mix of technical and theoretical concepts. The course on "Fundamentals of Cybersecurity" provides a comprehensive overview of computer and information security problems, fundamental cybersecurity concepts, principles, formal security models, information technology security hardware and software methods, and the ability standards, and to develop abilities to apply them. It covers various topics, including IT security problems, information security models, cryptography and secure methods of information coding, information and IT security standards and specifications, hardware security, identity management, OS security mechanisms, and file system security. The course is designed to equip students with the knowledge and skills to address the evolving cybersecurity challenges facing organizations today.

Identity and Access Management

The "Identity and Access Management" course is a key component of the cybersecurity curriculum, addressing the growing need for secure and efficient methods to manage digital identities in contemporary organizations. This course focuses on the principles, technologies, and practices necessary to safeguard access to critical digital assets, ensuring confidentiality, integrity, and availability. Students will explore the lifecycle of identity management, including identity creation, verification, and decommissioning, alongside modern access control mechanisms. The course emphasizes both theoretical foundations and practical applications.

Cyberattacks and Cyber Defenses: Tools and Methods

The CyberAttacks and CyberDefences course provides an in-depth understanding of cyber threats and defensive measures. It starts with an introduction to various cyberattacks and threats, explaining the CyberKillChain and the MITRE ATT&CK framework for analyzing adversary tactics. The course covers malware types and the concept of Defence in Depth, emphasizing multi-layered security strategies. Students learn about Cybersecurity Standards and ethical hacking techniques, including the OWASP Top Ten Attacks and common vulnerabilities like SQL injection and XSS. The course also delves into Penetration Testing, Red Teaming, Phishing as a Service, and WiFi security. In addition, it covers Network Security and Perimeter Defence, focusing on Layer 2 security, Next-Generation Firewalls (NGFW), IDS/IPS systems, and VPN technologies such as IPSec and OpenVPN. Key aspects of System Logging and Monitoring for detecting threats are explored, alongside strategies for managing cybersecurity incidents. The course concludes with an overview of CyberOperations and Security Operation Centers (SOC), along with SIEM/SOAR solutions and the growing role of AI in Cybersecurity to enhance threat detection and automated responses.

Cyber Security Management

This course will provide students with an overview of cybersecurity management principles. The participants will learn how to ensure confidentiality, integrity, and availability of secure assets, identify security risks, requirements, and countermeasures that mitigate these risks and implement the security requirements. The course is based on the well-established domain model for security risk management and principles of model-driven security. Security management will be illustrated by applying security management standards and patterns. Using the challenge-based learning approach, participants will explore security management challenges in business process-aware systems, intelligent infrastructure, distributed systems, risk-aware forensics-ready systems, and secure identity management systems.

PROJECT COORDINATOR

ktu kaunas university of technology

PROJECT PARTNERS

universidade de aveiro

Transilvania University of Brasov

https://www.cyberchallenge-erasmus.eu/

Kaunas University of Technology
Faculty of Informatics
Studentu str. 50, Kaunas, Lithuania