Cyber-physical Systems Institute			Semester 5. of the curriculum 2026-27-1			
Name of the subject:	Code of the subject:	Credits:	Weekly hours:			
				lec	sem	lab
IT Security	NBXIB1EBNF	5	full-time	2	0	2
Responsible person for the subject: Dr. Valéria PÓSER			Classification: associate professor			
Subject lecturer(s): Zsolt BRINGYE						
Prerequisites:	NKXOR1EBNF	Operating Systems				
Way of the assessment:	exam					

Course description	
Goal:	The main aim of the course is to develop a security-aware approach, to provide a comprehensive overview of IT security by introducing each area and to prepare future IT engineers to deal with IT security challenges that they will face in their future work.
Course description:	The main topics of the course are: A brief historical overview of IT security. Ethical issues, motivations, targets. security awareness, regulations. Cryptology, cryptographic algorithms and basic protocols. Vulnerability of workstations, servers, networks and infrastructures. Physical protection. Malware (malware). User authentication, privilege and access management. Operating systems password management. Password choice problems, password cracking. Network attack methods. Network perimeter protection (firewalls, IDS/IPS). PKI infrastructure. Communication security, Internet security protocols. Secure mail and data storage. Security of mobile platforms and cloud-based systems. Application vulnerability. Risk management.

Lecture schedule	
Education week	Topic
1.	LEC: Basic concepts of information security. Ethical issues. Legal regulations. LAB: Requirements. The test environment. Putting basic concepts into practice.
2.	LEC: Risk analysis, risk management. LAB: Risk management.
3.	LEC: Cryptography. Symmetric, asymmetric encryption, digital signature. LAB: Overview of risks and security measures on an example system.
4.	LEC: Overview of cryptographic algorithms. LAB: Encryption - historical basics.
5.	LEC: Password management. LAB: Encryption - server-side basics
6.	LEC: Malicious code, virus protection. LAB: Network security - border protection
7.	LEC: Network border security. LAB: Network security - DMZ, VPN
8.	LEC: Authentication, user identification. LAB: Operating Systems Security - AAA
9.	LEC: Public key infrastructure. LAB: Operating Systems Security - Group Policy
10.	LEC: Authorisation management. LAB: Exercise
11.	LEC: Safety Application Development, Web Application Security. LAB: User Security Awareness

12.	LEC: Data protection, data backup. LAB: Data backup and monitoring
13.	LEC: IoT Security LAB: Final paper
14.	LEC: Preliminary exam. LAB: Extra Final paper

Mid-term requirements	
Conditions for obtaining a mid-term grade/signature	The conditional of signature is the successful (at least satisfactory) completion of a final paper containing practical exercises and the submission of the mid-term assignment. Attendance of laboratory exercises is compulsory.

Assessment schedule	
Education week	Topic
13.	Practical ZH
14.	Preliminary exam Practical ZH retake, correction

Method used to calculate the *mid-term grade* (to be filled out only for subjects with mid-term grades)

-

Type of the replacement	
Type of the replacement of written test/mid-term grade/signature	In the case if the mid-term test does not reach 50%, the student can replace the test in the form of re-take test in the 14th week. Replacement of the mid-term mark: once in the first 10 working days of the examination period.

Type of the exam (to be filled out only for subjects with exams)

Students who meet the signature requirements during the semester (even during the last week) may take a
written preliminary examination at the last week.
Otherwise, they may take an oral examination during the examination period.

Calculation of the exam mark (to be filled only for subjects with exams)

The exam mark is determined on the basis of the written exam result or the written pre-exam mark and the performance of the mid-semester practicals (ZH, assignment, optional supplementary material test results)

Final grade calculation methods:

The final grade will be calculated using the following scale:

Achieved result	Grade
87% - 100%	excellent (5)
75%- 86%	good (4)
64% -74%	satisfactory (3)
51% - 63%	pass (2)
0 - 50 %	failed (1)

References

Obligatory:	Class materials published in Moodle

Recommended:	Computer and Information Security Handbook by John R. Vacca (Author), John Vacca MSc and MBA (Editor)
Other references:	