Obuda University John von Neumann Faculty of Informatics			Institute of Cyberphysical Systems	
Name and code: IT Security, NIEIB0EBNE			**Credits*: 4*** *2022/23 year II. semester*	
Subject lecturers: Ernő Rigó, Zsolt Bringye				
Prerequisites (with code):				
Weekly hours:	Lecture: 2	Seminar.: 0	Lab. hours: 2	Consultation: 0
Way of assessment:	Exam			

Course description:

Goal: The goal of the subject is to raise security awareness, to provide an overview on certain areas of IT security, and to prepare the prospective computer engineer for IT security problems, which arise in their later work.

Course description: Short overview on the history of information security. Ethical issues, motivations, targets, security awareness, regulations. Cryptology, cryptographic algorithms and basic protocols. Vulnerability of workstations, servers, networks and infrastructures. Physical protection. Malicious software (malware). User authentication, authorization and access management. Password management in operating systems. Problems of password choice, password breaking techniques. Network attack methods. Border protection of network (firewalls, IDS/IPS). Public Key Infrastructure. Secure communication, internet security protocols. Secure mail and data storage. Security of mobile and cloud-based systems. Vulnerability of applications. Risk management.

Lecture schedule

Education week	*Topic*
1.	Lecture: The fundamental concepts of the information security. The CIA triad and the Parkerian hexad.
2.	Lecture: Short history of Cryptography. Basic methods of cryptanalysis. Classical algorithms.
3.	Lecture: Symmetrical crypto algorithms, AES
4.	Lecture: Asymmetric encryption, hash, digital signature
5.	Lecture: Identification and Authentication. Factors, multifactor authentication. Passwords.
6.	Lecture: Authorization methods
7.	Lecture: Risk management – Risk factors: physical, human, technical.
8.	Lecture: Risk management process and methods
9.	Lecture: Malwares
10.	Lecture: Data rescue, data protection
11.	Lecture: e-mail security
12.	Lecture: Border protection, firewall, IDS/IPS
13.	Lecture: PKI
14.	Lecture: Laws, regulations and standards

Midterm requirements

Both midterm exams (labs) are successful (at least 50 % both of them).
The student has to appear on the lectures and labs.

Final grade calculation methods

Achieved result	Grade
86%-100%	excellent (5)
74%-85<%	good (4)
62%-73<%	average (3)
50%-61<%	satisfactory (2)
0%-49<%	failed (1)

Type of exam

Written exam

Type of replacement

References

Mandatory:
Lecture notes (download form https://elearning.uni-obuda.hu/)

Recommended:

- Security Engineering: A Guide to Building Dependable Distributed Systems 2nd Edition by Ross J. Anderson
- Applied Cryptography: Protocols, Algorithms and Source Code in C 1st Edition by Bruce Schneier
- The Basics of Information Security, Second Edition: Understanding the Fundamentals of InfoSec in Theory and Practice 2nd Edition by Jason Andress