Course Unit Descriptor

Study Programme: Information Technology Management

Course Unit Title: Data Security

Course Unit Code: OAS219

Name of Lecturer(s): Associate Professor Dalibor Dobrilović, PhD

Type and Level of Studies: Bachelor Academic Degree

Course Status (compulsory/elective): Compulsory

Semester (winter/summer): Winter

Language of instruction: English

Mode of course unit delivery (face-to-face/distance learning): Face-to-face

Number of ECTS Allocated: 7

Prerequisites: None

Course Aims:

The main goal of the course is to teach students about corporate information security through data security concepts and understanding cryptography, security protocols and technologies as well. The additional goal is to teach students about the risks at all levels and data and systems protection methods that should be implemented.

Learning Outcomes:

Upon successful completion of the course, it is expected that the students will master the concepts of data security and protection. The practical training will give students practical knowledge about detection, prevention, and neutralization of attacks on data and system security.

Syllabus:

Theory

The introduction to corporate and information security. Types of attacks: passive attacks, active attacks, malicious programs, denial of services. Basic cryptography concepts, keys, and encryption algorithms. Encryption with the public key and hash functions, digital signature, digital certificates. Applications for security and protection of computer systems. Network tools and security applications: Authentication applications (Kerberos and X.509 authentication directories service); Protection and security of e-mail (PGP, S / MIME, DKIM); Transport layer security (SSL, TLS) and IP security (IPSec, transport mode, tunneling mode, AH and ESP). Network barriers (packet filtering, NAT, Circuit level gateways on the layer, ALG or Application layer gateway on the application layer, DNS sharing, SSH). Web security (SSL, TLS, digital "watermark," SET). VPN protection. WLAN protection systems: access control, an extended protocol for EAP authentication, security techniques (WEP, WPA, WPA2, IEEE 802.11i). Cloud computing systems security.

Practice

Practical work covers laboratory exercises with solving tasks and practical problems, with the application of simulation software and systems and network devices.

Required Reading:

1. W. Stallings, Cryptography and Network Security, sixth edition, Prentice Hall, 2012.

2, W. Stallings, L. Brown, Computer Security: Principles and Practice, Prentice Hall, 2012.

Weekly Contact Hours: 4	**Lectures:** 2	**Practical work: 2**

Teaching Methods:

Lectures and students group work

Knowledge Assessment (maximum of 100 points): 100			
Pre-exam obligations	points	**Final exam**	points
Active class participation	10	oral exam	40
Preliminary exam(s)	30		
Seminar(s)	20		