COURSE OUTLINE

1. GENERAL INFORMATION

FACULTY	ECONOMY AND MANAGEMENT		
DEPARTMENT	ORGANIZATIONS MANAGEMENT, MARKETING AND TOURISM		
LEVEL OF STUDY	UNDERGRADUATE		
COURSE CODE	**1605-230713**	**SEMESTER**	**7th (dir. Marketing)**
TITLE	**Information Systems Security and Privacy Protection**		

Autonomous Teaching Activities	**WEEKLY TEACHING HOURS**	**CREDITS**
Lectures	3	5

COURSE TYPE	GENERAL KNOWLEDGE SPECIALIZATION
PREREQUISITE COURSES	NONE
TEACHING LANGUAGE	GREEK AND ENGLISH
COURSE OFFERED TO ERASMUS STUDENTS	YES
COURSE WEBPAGE (URL)	

2. LEARNING OUTCOMES

Learning outcomes

The course gives the basic concepts for cryptography and how these concepts are used in general in the security of computer systems.

Upon successful completion of the course students will be able to:

1. KNOWLEDGE: fully describe all the basic concepts necessary for understanding cryptography and computer systems security
2. UNDERSTANDING: identify the main risks of personal data security and privacy breach
3. APPLICATION: examine the principles and effectiveness of the most well-known data protection methods.
4. ANALYSIS: combine different applications of information security techniques in the information systems of a company or an organization and develop them.
5. COMPOSITION: create and compose the Security Plan of an Information System
6. EVALUATION: compare and evaluate case studies.

General Skills

- Search, analysis and synthesis of data and information, using the necessary technologies
- Autonomous Work
- Teamwork
- Exercise criticism and self-criticism
- Promoting free, creative, and inductive thinking

•Decision making

3. COURSE CONTENT

1. Introductory security concepts. Review of cryptography concepts.
2. Attack models.
3. Identification. Security entrance check.
4. Database security.
5. Network-level security. Transport level security.
6. Security at the application level.
7. Domain name security. Wireless network security.
8. Perimeter security (Firewalls, intrusion control systems, etc.).
9. Malware.
10. Software security.
11. Operating systems security.
12. Security management and standards (e.g., ISO 27000).
13. Legal issues of network and systems security.

4. TEACHING AND LEARNING METHODS - ASSESSMENT

TEACHING METHOD	Face to Face	
ICT USE	Use of modern teaching methods by electronic means (where required). Learning process support through the electronic platform e-class.	
TEACHING ORGANIZATION	***Activities***	***Working Load per Semester***
	Lectures	39
	Practice Exercises	25
	Bibliographic study and analysis	30
	Progress	15
	Self-study	51
	TOTAL	150
ASSESSMENT	Written final exam (100%) that includes: • Theoretical open-ended questions • Issues of analytical approach and thinking • Multiple choice questions The test material is posted on Moodle and, before the test, time is spent on answering questions about the test material. A file of students' examination documents is kept until they receive their degree. After the exam, time is available to each student to clarify his / her mistakes and explain his / her grade.	

5. REFERENCES

-Suggested bibliography:

- Information & Systems Security in Cyberspace, S. Katsikas, S. Gritzalis, K. Lambrinoudakis, 2020, New Technologies Publications
- Cryptography and network security: principles and applications, W. Stallings, 2011, Ion,
- Basic Network Security Principles: Applications and Standards, W. Stallings, 2008, Key Number,
- Computer Security: Principles and Practices, W. Stallings, L. Brown, 2016, Key Issue, ISBN: 978-960-461-668-8.