

## COURSE OUTLINE

### (1) GENERAL

<b>SCHOOL</b>	Engineering		
<b>ACADEMIC UNIT</b>	Industrial Design and Production Engineering		
<b>LEVEL OF STUDIES</b>	Undergraduate		
<b>COURSE CODE</b>	<b>9010</b>	<b>SEMESTER</b>	<b>9</b>
<b>COURSE TITLE</b>	Data Security and Protection		
<b>INDEPENDENT TEACHING ACTIVITIES</b>		<b>WEEKLY TEACHING HOURS</b>	<b>CREDITS</b>
Theory (Lectures)		3	3
Tutorial/Project		0.5	1
Laboratory		0.5	1
		<b>4</b>	<b>5</b>
<b>COURSE TYPE</b>	Specialized general knowledge, skill development		
<b>PREREQUISITE COURSES:</b>	No		
<b>LANGUAGE OF INSTRUCTION and EXAMINATIONS</b>	Greek		
<b>IS THE COURSE OFFERED TO ERASMUS STUDENTS</b>	Yes (in English)		
<b>COURSE WEBSITE (URL)</b>	<a href="https://eclass.uniwa.gr/courses/IDPE324/">https://eclass.uniwa.gr/courses/IDPE324/</a>		

## (2) LEARNING OUTCOMES

<b>Learning outcomes</b>
<p>The course covers the general part of the scientific area of Data Security and Protection. The aim of the course is to create a very broad framework of theoretical and practical knowledge, which will equip the student for the labor market in the field of Security in Information Technology.</p> <p>Upon successful completion of this course, the student will:</p> <ul style="list-style-type: none"><li>• know the problems of security and data protection in Information and Communication Systems as well as the distinction of data into sensitive, personal and private,</li><li>• recognize the vulnerabilities of information and communication systems,</li><li>• be able to apply basic security policy design principles,</li><li>• know the features and security mechanisms that implement these policies (such as anonymity, encryption, etc.),</li><li>• be familiar with examples that implement and apply security mechanisms in different Operating Systems,</li><li>• have knowledge of Database Security,</li><li>• know the different types of firewalls and how they are used and implemented,</li><li>• be aware of authentication mechanisms, their role and importance,</li><li>• be familiar with Computer Forensics and will be familiar with the tools that support them,</li><li>• understand cryptography and cryptanalysis, and finally,</li><li>• have understood the Intrusion Detection Systems, how they work and the techniques used in them</li></ul>
<b>General Competences</b>
<ul style="list-style-type: none"><li>• Search for, analysis and synthesis of data and information, with the use of the necessary technology</li><li>• Working independently</li><li>• Team work</li><li>• Decision-making</li><li>• Working in an interdisciplinary environment</li><li>• Production of new research ideas</li><li>• Production of free, creative and inductive thinking</li></ul>

## (3) SYLLABUS

<ul style="list-style-type: none"><li>• General Information Security Issues in Information Technology (IT Security)</li><li>• Cryptography (mechanisms, algorithms, public encryption systems)</li><li>• Operating Systems Protection (Operating Systems Protection)</li><li>• Database Security (Data Base Security)</li><li>• Access Control</li><li>• Network and Distributed Systems Security</li><li>• Internet Security</li><li>• Attack Detection</li><li>• Computer Forensics</li><li>• Blockchain Technologies</li><li>• Risk Analysis</li><li>• Security Management</li><li>• Legal and Ethical Issues (GDPR)</li></ul>
---

#### (4) TEACHING and LEARNING METHODS-EVALUATION

<b>DELIVERY</b>	<ul style="list-style-type: none"> <li>• Lectures</li> <li>• Practical Exercises</li> <li>• Assignments-Presentations</li> </ul>	
<b>USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGY</b>	Use of ICT in teaching, laboratory education in submission of assignments and communication with students	
<b>TEACHING METHODS</b> <i>The manner and methods of teaching are described in detail.</i> <i>Lectures, seminars, laboratory practice, fieldwork, study and analysis of bibliography, tutorials, placements, clinical practice, art workshop, interactive teaching, educational visits, project, essay writing, artistic creativity, etc.</i>  <i>The student's study hours for each learning activity are given as well as the hours of non-directed study according to the principles of the ECTS</i>	<b>Activity</b>	<b>Semesterworkload</b>
	Lectures	40
	Assignments	50
	Personal study	60
		<b>Course total (30h/ECTS)</b>
<b>STUDENT PERFORMANCE EVALUATION</b> <i>Description of the evaluation procedure</i>  <i>Language of evaluation, methods of evaluation, summative or conclusive, multiple choice questionnaires, short-answer questions, open-ended questions, problem solving, written work, essay/report, oral examination, public presentation, laboratory work, clinical examination of patient, art interpretation, other</i>  <i>Specifically-defined evaluation criteria are given, and if and where they are accessible to students.</i>	<p><b>Language of Assessment</b> Greek</p> <p><b>Description</b> Written exams, laboratory evaluation and project evaluation</p> <p><b>Student assessment methods</b> Language of evaluation : Greek or English</p> <p>Methods of evaluation for theory</p> <ul style="list-style-type: none"> <li>- Final written exam with problem solving (60%)</li> <li>- Public Presentation (40%)</li> </ul> <p>Methods of evaluation:</p> <ul style="list-style-type: none"> <li>• Written Exam: 60%</li> <li>• Assignment: 40%</li> </ul> <p>The assessment criteria are announced to students at the beginning of the semester and are published on the course webpage in the e-Class platform.</p>	

#### (5) ATTACHED BIBLIOGRAPHY

**- Suggested bibliography:**

- Σουρής Α., Πατσός Δ., Γρηγοριάδης Ν., Ασφάλεια της Πληροφορίας, ΕΚΔΟΣΕΙΣ ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ ΜΟΝ. ΕΠΕ, 2004, ISBN: 960-8105-66-8. 5. Κάτσικας Σ.Κ., Γκρίτζαλης Δ.,
- Γκρίτζαλης Σ., Ασφάλεια Πληροφοριακών Συστημάτων, Εκδόσεις Νέων Τεχνολογιών, 2004
- Stallings και Brown, Ασφάλεια Υπολογιστών: αρχές και Πρακτικές, 2016, ΕΚΔΟΣΕΙΣ ΚΛΕΙΔΑΡΙΘΜΟΣ ΕΠΕ, ISBN: 978-960-461-668-8.
- Γκρίτζαλης Σ., Γκρίτζαλης Δ., Κάτσικας Σ., Ασφάλεια Δικτύων Υπολογιστών, Α. ΠΑΠΑΣΩΤΗΡΙΟΥ & ΣΙΑ ΟΕ, 2003, ISBN: 978-960-7530-45-5.
- Stallings, Κρυπτογραφία για Ασφάλεια Δικτύων Αρχές και Εφαρμογές, ΜΑΡΙΑ ΠΑΡΙΚΟΥ & ΣΙΑ ΕΠΕ, 2011, ISBN: 9789604117307.

**- Related academic journals:**

- International Journal of Information Security, Springer
- IEEE Transactions on Information Forensics and Security
- IEEE CyberSecurity