Cybersecurity Protocols and Standards

1. GENERAL

SCHOOL	ENGINEERING		
DEPARTMENT	INFORMATICS AND COMPUTER ENGINEERING		
LEVEL OF STUDY	POSTGRADUATE (7)		
MSc Program	CYBERSECURITY		
COURSE UNIT CODE	**CSCYB102**	**SEMESTER OF STUDY**	1st
COURSE TITLE	**Cybersecurity Protocols and Standards**		

COURSEWORK BREAKDOWN	**TEACHING WEEKLY HOURS**	**ECTS Credits**
Lectures	3	
Problem Solving- Research	2	
Tutorials		
	5	**7**

COURSE UNIT TYPE	COMPULSORY
PREREQUISITES :	NONE
LANGUAGE OF INSTRUCTION/EXAMS:	GREEK, ENGLISH
MODULE WEB PAGE (URL)	UNIWA Open eClass | ΚΑΝΟΝΕΣ και ΠΡΩΤΟΚΟΛΛΑ ΚΥΒΕΡΝΟΑΣ...

2. LEARNING OUTCOMES

Learning Outcomes

The course learning outcomes, specific knowledge, skills and competences of an appropriate level, which the students will acquire with the successful completion of the course are described.

Consult Appendix A

- *Description of the level of learning outcomes for each qualifications cycle, according to the Qualifications Framework of the European Higher Education Area*
- *Descriptors for Levels 6, 7 & 8 of the European Qualifications Framework for Lifelong Learning and Appendix B Guidelines for writing Learning Outcomes*

Students can

- understand the purpose, scope, and importance of various standards
- memorize key terms, definitions, and foundational principles of cybersecurity standards. This level helps build a fundamental understanding of security concepts cybersecurity standards.
- analyze the structure, components, and requirements of cybersecurity standards
- Evaluate cybersecurity standards, considering their strengths, weaknesses, and relevance to specific organizational needs.
- Apply cybersecurity standards to real-world situations
- Describe, the methods used for a protocol launch
- Demonstrate, the ability to select the appropriate protocol
- Modify a protocol in order to update its contents
- Compare, similar protocols
- Develop from scratch a protocol with all the responsible committees
- Decide, on the protocol selection for a given task to undertake

General Skills

Taking into consideration the general competences that the degree-holder must acquire (as these appear in the Diploma Supplement and appear below), at which of the following does the course aim?

Search for, analysis and synthesis of data and information, with the use of the necessary technology *Adapting to new situations* *Decision-making* *Working independently* *Team work* *Working in an international environment* *Working in an interdisciplinary environment* *Production of new research ideas*	*Project planning and management* *Respect for difference and multiculturalism* *Respect for the natural environment* *Showing social, professional and ethical responsibility and sensitivity to gender issues* *Criticism and self-criticism* *Production of free, creative and inductive thinking* *Others*

Recall basic facts and concepts related to cybersecurity standards
Use cybersecurity standards in specific contexts or scenarios
Examine and break down cybersecurity standards to understand their components.
Assess the effectiveness and appropriateness of cybersecurity standards Develop innovative solutions or strategies based on cybersecurity standards.
Comprehend the meaning and significance of cybersecurity standards.

3. COURSE CONTENTS

The description contains the material to be covered during the 13 sessions.

1) Description of Protocols and Standards
2) Leading Organisations in Cybersecurity protocols, The hierarchy in protocol production
3) BOT Basics, Automotive Protocols (e.g. FlexRay, SAE J2735)
4) Telecommunication Protocols
5) Cybersecurity Maritime Protocols and Standards, AI ethics code
6) FIPS, ILIT
7) Governance Risk and Compliance (ERNEST YOUNG) and Trusted Computer Security
8) GDPR, Protection of Personal Data GRC ()
9) CERT, NIST, NIS, NERC
10) Common Criteria (ISO 15408) and Orange Book
11) Network protocols
12) Mobile Cybersecurity Protocols and standards
13) Hospital Cybersecurity protocols and standards

4. TEACHING METHODS - ASSESSMENT

MODE OF DELIVERY	Face to face
USE OF INFORMATION AND COMMUNICATION TECHNOLOGY	**Using interactive notes and slides to demonstrate the basic functionality of digital systems**
TEACHING METHODS	

Method description	*Semester Workload*
Lectures	39
Tutorials	26
Research work	50
Self study	60
Total course hours (25 h workload per ECTS)	***175***

ASSESSMENT METHODS	II. Multiple choice questions (40%) III. Class Participation (20%) IV. Research work on a standard (40%)

5. RESOURCES

Recommended Books:

1) *Cybersecurity Risk Management - Mastering the Fundamentals Using the NIST, Cynthia Brumfield, Brian Haugli, WILEY, 2021*
2) *5G Cybersecurity Standards, ENISA, 2022*
3) *"NIST 800-53: Security and Privacy Controls for Federal Information Systems and Organizations" by Ron*

Ross, Stu Katzke, Arnold Johnson, National Institute of Standards and Technology, 2020

4) *ISO 27001/27002: A Pocket Guide" by Alan Calder, IT Governance Publishing, 2008*

5) *CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide" by Mike Chapple, James Michael Stewart, and Darril Gibson, 7th ed. John Wiley and Sons, 2015*

6) *Cybersecurity for Hospitals and Healthcare Facilities, Ayala Luis, Apress, 2016*

7) *Biometric-Based Physical and Cybersecurity Systems, Obaidat, Traore, Wouhgang (eds), Springer Nature Switzerland AG, 2018*

8) *Effective Cybersecurity: a Guide to Using Best Practices and Standards, William Stallings, 2018*

9) *Automotive Cyber Security: Introduction, Challenges, and Standardization, Kim S., Shrestha R., Springer,2020*

10) *The Ultimate Guide to Cybersecurity Planning for Businesses, 2020*

11) *Derived Test Requirements for FIPS PUB 140-2: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (Author), 2011*

12) *Cybercrime and Cyber Warfare, Igor Bernik, ISTE Ltd and John Wiley & Sons Inc,2013*

13) *Cyber Security Essentials, Rick Howard, Taylor & Francis Inc, 2010*

Webliography

https://www.itgovernanceusa.com/cybersecurity-standards

https://www.enisa.europa.eu