Course Title	Communications and Network Security				
Course Code	CYS610				
Course Type	Compulsory				
Level	Master (2nd cycle)				
Year / Semester	1st Year / 1st Semester				
Teacher's Name	TBA				
ECTS	7	Lectures / week	3 Hours	Laboratories / week	None
Course Purpose and Objectives	This course introduces fundamental concepts of communications and network security, particularly in the context of internal and external threats to the operation of the network and to the devices that are attached to it.				
Learning Outcomes	Upon succesful completion of this course students should be able to: • Describe the underlying principles of networking layers, architecture, topologies, protocol stacks, separation of duties. • Explain the basic types of networking device, both logical and physical. • Analyse networking methods and applications in practical systems. • Classify and describe different types of wired network attacks. • Classify and describe different types of wireless network attacks. • Describe and evaluate methods and devices used to protect networks.				
Prerequisites	None	Co-requisites	None		
Course Content	Introduction: Refresh on fundamental networking principles and devices, OSI and TCP/IP models. Different types of networking areas – WAN, LAN, MAN, PAN, wireless and mobile systems. Principles: the network as a route for cyberattacks, how the network can be protected, vulnerabilities, threats. Network Attacks: scanning, malware, (D)DoS, route poisoning, MAC spoofing, sniffing, authentication attacks, man-in-the-midde, session takeover, wiretaps, MAC table flooding, ARP poisoning, ICMP attacks, DNS poisoning, smurf and fraggle attacks, phishing, spam, war-dialing,				

	methods to prevent the network attacks that have been covered (within the discussion of each attack type). Wireless Attacks: Encryption and key management vulnerabilities, wireless sniffing, war-driving, mobile/cellular cell spoofing, eavesdropping, mobile phone attacks, methods to prevent the network attacks that have been covered (within the discussion of each attack type). General protection, prevention and detection: Firewalls and packet filtering, demilitarized zones (DMZ), intrusion detection and prevention systems, IPsec, VLANs and network zoning, MAC access control, network authentication, system hardening, encryption, authentication, universal threat management (UTM), web filtering, honeypots, awareness. Network management as an effective information gathering tool and starting point for comprehensive protection mechanisms, use of network and asset management tools to ensure uniform conformity to relevant cybersecurity standards and policies. Business case study and lecture: Lecture by invited experts from the cybersecurity industry. Discussion normally focuses on usual network attacks and methods for protection.
Teaching Methodology	Face – to – face
Bibliography	*"Computer Networks (5th Edition)"*, by Andrew S. Tanenbaum and David J. Wetherall *"Network and System Security, Second Edition"*, by John R. Vacca *"Network Security Essentials: Applications and Standards (5th Edition)"*, by William Stallings IEEE Journals and Magazines
Assessment	Examinations 60% Assignment(s) 40% 100%
Language	English