Discipline	COMPUTER AND NETWORK SECURITY code: 46/47/48-13 **summer semester**	
Specialty	Computer Systems and Technologies	
ECTS credits: **7**	Form of assessment: exam	
Lecturer	Assoc. Prof. Hristo Valchanov, PhD Room 207 – 4 E Phone: +359 52 383 278; 439 E-mail: hristo@tu-varna.bg	
Department	Computer Science and Engineering	
Faculty	Faculty of Computing and Automation	

Learning objectives:

The main objective of the course is to provide students with knowledge and skills to assess the security risk of a computer network. The types of attacks and malicious code that cause inaccessibility or degradation of the quality of network services are considered. Students are acquainted with the current standards and current law in Bulgaria concerning the security of the data transmitted on the Internet. Modern networking solutions and network and information security solutions are analyzed to achieve optimal modularity, robustness, flexibility, security and ease of management. The potential breakthroughs in the network structure are shown.

CONTENTS:

Training Area	Hours lectures	Hours seminar exercises
International standards concerning the security of computer networks. Stages and activities to build a network security management system.	2	2
Security of classified information networks - basic principles and requirements. Major vulnerabilities. Risk - nature, detection, risk assessment, risk minimization mechanisms.	2	2
Security of the OS. Linux Security Model. Windows Server Security Model. Protect files and directories. Access control to objects.	2	2
Security of the OS. Malware - viruses, worms, Trojans. Detection and protection. Buffer overflow attack.	2	2
TCP / IP protocol stack vulnerabilities. IP Spoofing and Denial of Service attacks (DoS).	2	2
Attacks against DNS. Vulnerabilities of Zone Transfer and Dynamic Updates. DNS Cache Poisoning Attack.	2	2
Port Scan- Nmap. Vulnerability Scanning - Nessus. Passive packet monitoring. Intrusion Detection Systems (IDS).	2	2
Packet filtering - Iptables	2	2
Enterprise Information Security Solutions. Firewalls - Purpose, Functionality, Classification.	2	2
Vulnerabilities of authentication. Dictionary Attacks. Breaking passwords with Rainbow Tables. Password-by-pass schemes. RADIUS protocol.	2	2

Bots and botnets. Distributed DoS Attacks.	2	2
Security issues in Peer-to-Peer networks (P2P). Wireless network security.	2	2
Web security. SQL injection attack. Web scams (fishing). Clickjacking. Security in virtualization and cloud services.	2	2
TOTAL: 60 h	**30**	**30**