1.	Course title	Computer Systems Security		
2.	Course code			
3.	Study program	All		
4.	Unit offering the course	**FCSE**		
5.	Undergraduate/postgraduate/PhD	**Undergraduate**		
6.	Year/semester 3-4/Summer/Elective	7. ECTS: **6**		
8.	Teacher(s)	Acad. Prof. Ljupcho Kocarev, Assist. Prof. Vesna Dimitrova, Assist. Prof. Sonja Filiposka, Assist. Prof. Boro Jakimovski, Assist. Prof. Anastas Mishev, Assist. Prof. Igor Mishkovski		
9.	Course prerequisites	Operating Systems		
10.	Goals (competences): Introduction to procedures and mechanisms for protection of computer systems from security point of view and procedures for increasing the level of computer system security against unauthorized access.			
11.	Course content: Need for security of computer systems. Introduction and basic concepts. Ethical standards and responsibility. Basic concepts of cryptography. Examples of protocols for encryption. Secret key encryption. Public key encryption. Attacks of encrypted systems. Basic secure mechanisms in operating systems. Architecture of secure operating systems, authentication, access control: access lists, implementation of access control (Unix, Java), Bell and La Padula model. Operating system mechanisms for supporting MAC policies. Security Policies Clark-Wilson and Chinese Wall. Weaknesses of security in operating systems. Security of Internet protocols. Web security. Security network management. Secure mechanisms in TCP/IP based networks and in DNS. Malicious software. Firewalls. Detection of viruses, Trojan horses. Unauthorized attempts to login. Spam (via e-mail subsystem). Secure in smart cards and other types of cards. Protocols for secure electronic transactions, security in communication programs. Database security.			
12.	Teaching methods: Lectures, trainings, individual work, project, seminar work.			
13.	Total available time	6 ECTS x 30 hours = 180 hours		
14.	Distribution of the available time	30+45+25+40+40 = 180 hours		
15.	Teaching activities	15.1.	Lectures	30 hours
		15.2.	Training (labs, problem solving), seminar and team work	45 hours
16.	Other activities	16.1.	Project work	25 hours
		16.2.	Self study	40 hours
		16.3.	Home work	40 hours
17.	Grading			

	17.1.	Tests	80 points
	17.2.	Seminar work/project (written or oral presentation)	10 points
	17.3.	Active participation	10 points
18.	Grading criteria	to 49 points	5 (five) (F)
		from 50 to 59 points	6 (six) (E)
		from 60 to 69 points	7 (seven) (D)
		from 70 to 79 points	8 (eight) (C)
		from 80 to 89 points	9 (nine) (B)
		from 90 to 100 points	10 (ten) (A)
19.	Final exam prerequisites	Successful completion of activities 15 and 16	
20.	Course language	Macedonian and English	
21.	Quality assurance methods	Internal evaluation mechanisms supported by student polls	

22. Literature

22.1. Compulsory

No.	Authors	Title	Publisher	Year
1.	Dietter Gollman	Computer Security	John Wiley & Sons	1998
2.	Bruce Schneier	Applied Cryptography Second Edition: protocols, algorithms, and source code in C	John Wiley & Sons	1996
3.	William Stalings	Cryptography and network security – Principles and Practice	Prentice hall	2003

22.2. Mandatory

No.	Authors	Title	Publisher	Year
1.	Mark Stamp	Information security – principles and practice	John Willey and Sons	1991
2.				
3.				