1.	Course title	**Computer networks security**		
2.	Course code	KMET-I-11		
3.	Study program	**Computer networks and e-technologies**		
4.	Unit offering the course	**FCSE**		
5.	Undergraduate/master/PhD	**Master**		
6.	Year/semester 1(2)/summer/elective	7. ECTS: **6**		
8.	Teacher(s)	Prof. Ljupco Kocarev		
9.	Course prerequisites	None		
10.	Goals (competences): After successfully completing the course, the student is expected to have advanced knowledge in the field of network and computer security. The student will be able to apply the knowledge in practice in various types of networking systems especially for security of critical data (e.g. in banks).			
11.	Course content: Introduction. Ethical norms and responsibility. Encryption structure. Encryption protocols. Secret key encryption. Public key encryption. Hacking encrypted systems. Basic protection mechanisms on the operating system level. Security system architecture on the operating system level. Authentication, access control: access list control, access control implementation (Unix, Java), Bell and La Padula models. Operating system mechanisms for MAC policy support. Security policies: Clark-Wilson and China wall. Operating systems weaknesses. Secure kernels. Security mechanisms for TCP/IP based networks and DNS-sec. Firewalls. Virus detection, Trojan horses, unauthorised login attempts. Spam. Agents and mobile codes. Smart card security. Electronic transactions security protocols. Student projects.			
12.	Teaching methods: Lectures supported by slide presentations, interactive lectures, trainings (using lab equipment and software packages), team work, case studies, invited guests and lectures, individual practical assignments presentations, seminar paper, e-learning (forums, consultations).			
13.	Total available time	6 ECTS x 30 hours = 180 hours		
14.	Distribution of the available time	30 + 15 + 135 = 180 hours		
15.	Teaching activities	15.1.	Lectures	30 hours
		15.2.	Training (labs, problem solving), seminar and team work	15 hours
16.	Other activities	16.1.	Project work	60 hours
		16.2.	Self study	25 hours
		16.3.	Home work	50 hours
17.	Grading			
	17.1.	Tests		45 points
	17.2.	Seminar work/project (written or oral presentation)		45 points
	17.3.	Active participation		10 points
18.	Grading criteria	to 59 points		5 (five) (F)

				from 60 to 68 points	6 (six) (E)	
				from 69 to 76 points	7 (seven) (D)	
				from 77 to 84 points	8 (eight) (C)	
				from 85 to 92 points	9 (nine) (B)	
				from 93 to 100 points	10 (ten) (A)	
19.	Final exam prerequisites			Successfully completed activities 15.1 and 15.2		
20.	Course language			Macedonian and English		
21.	Quality assurance methods			Internal evaluation and student questionnaires		
22.	Literature					
	22.1.	Compulsory				
		No.	Authors	Title	Publisher	Year
		1.	M. Whitman, H. Mattord	Principles of Information Security	Thomson Course Technology	2009
		2.	B. Graham, D. Dodd	Security Analysis, 6th Edition	McGraw-Hill	2009
		3.	R. Anderson	Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition	Wiley Publishing	2008
	22.2.	Additional				
		No.	Authors	Title	Publisher	Year
		1.		Selected papers		
		2.				
		3.				