professor Simona Samardzhiska 9. Course enrollment prerequisites Оперативни системи 10. Course program goals (competencies): Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security. 11. Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptogra Public key cryptography, Hash functions) Cryptographic Algorithms (Types Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryp Schemes) Basic Authentication Terms (Authentication, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols with symme cryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Otv Rees, Needham-Schroeder, Public Key Infrastructure) Real Protocols (SSH, SSL / T Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Secu Functions, Trusted OS) 12. Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and software)	1.	Course Title Information security								
4. Study Program Organizer Faculty of Computer Science and Engineering 5. Degree (first, second, third cycle) first cycle 6. Academic year / semester 7. ECTS credits 6 Academic year / semester 7. ECTS credits 6 Academic year / semester 7. ECTS credits 6 B Teacher associate professor Vesna Dimitrova, assis professor Simona Samardzhiska 9. Course enrollment prerequisites Oneparuвни cucreми 10. Course program goals (competencies): Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security. 11. Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryp Schemes) Basic Authentication Terms (Authentication, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication models (Multilevel security models, Covert channels, Firewalls, systems) Brotocols (Simple protocols, Key exchange protocols (SSH, SEL / Ti Open SSL, Zero-Knowledge Protocols, Key Infrastructure) Real Protocols (SSH, SSL / Ti Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Security of Malicious Software, Software Attacks) Operating Systems Security (OS Security Na	2.	Code	F18L3W043							
5. Degree (first, second, third cycle) first cycle 6. Academic year / semester 3 / winter / optional 7. ECTS credits 6. Teacher associate professor Vesna Dimitrova, assis professor Simona Samardzhiska 9. Course enrollment prerequisites Оперативни системи 10. Course program goals (competencies): Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security. 11. Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptogra Public key cryptography, Hash functions) Cryptographic Algorithms (Types Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryp Schemes) Basic Authentication Terms (Authentication, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols with symme cryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Otv Rees, Needham-Schroeder, Public Key Infrastructure) Real Protocols (SSH, SSL / Ti Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Secu Functions, Trusted OS) 12. Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and softw packages), teamwork, case studies, invited guest lecturers, independent preparation de	3.	Study program	Software engineering and information systems							
6. Academic year / semester 3 / winter / optional 7. ECTS credits 6. Teacher associate professor Vesna Dimitrova, assis professor Simona Samardzhiska 9. Course enrollment prerequisites Oneparuвни системи 10. Course program goals (competencies): Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security. 11. Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptogra Public key cryptography, Hash functions) Cryptographic Algorithms (Types Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication) Basic Authorization Terms (Authorization, Access control matri Authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols (SSH, SSL / TI Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Sect Functions, Trusted OS) 12. Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and softw packages), teamwork, case studies, invited guest lecturers, independent preparation defense of a project assignment and seminar work. 13. Total available time 6 ECTS x 30 hours = 180 hours	4.	Study Program Organizer	Faculty of Computer Science and Engineering							
3 / winter / optional 6 8. Teacher associate professor Vesna Dimitrova, assis professor Simona Samardzhiska 9. Course enrollment prerequisites Оперативни системи 10. Course program goals (competencies): Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security. 11. Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptography Basic Cryptography, Hash functions) Cryptographic Algorithms (Types Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication) Basic Authorization Terms (Authentization, Access control matri Authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols with symmetryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Str T: Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Securitorios, Trusted OS) 12. Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and softw packages), teamwork, case studies, invited guest lecturers, independent preparation defense of a project assignment and seminar work. 13. Total available time 6 ECTS x 30 hours = 180 hours	5.	Degree (first, second, third cycle)	first cycle							
9. Course enrollment prerequisites Оперативни системи 10. Course program goals (competencies): Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security. 11. Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryp Schemes) Basic Authentication Terms (Authentication, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols with symmetryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Otv Rees, Needham-Schroeder, Public Key Infrastructure) Real Protocols (SSH, SSL / T: Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (T) of Malicious Software, Software Attacks) Operating Systems Security (OS Security of Malicious Software, Software Attacks) Operating Systems Security (OS Security of Malicious Software, Software Attacks) Operating Systems Security (OS Security is packages), teamwork, case studies, invited guest lecturers, independent preparation defense of a project assignment and seminar work. 12. Learning methods: 13. Total available time	6.									
10. Course program goals (competencies): Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security. 11. Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptogra Public key cryptography, Hash functions) Cryptographic Algorithms (Types Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryp Schemes) Basic Authentication Terms (Authentication, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication) Basic Authorization Terms (Authorization, Access control matri Authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols with symmed cryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Otv Rees, Needham-Schroeder, Public Key Infrastructure) Real Protocols (SH, SSL / TU Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Secu Functions, Trusted OS) 12. Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and softv packages), teamwork, case studies, invited guest lecturers, independent preparation defense of a project assignment and seminar work. 13. Total available time 6 ECTS x 30 hours = 180 hours	8.	Teacher	associate professor Vesna Dimitrova, assistant professor Simona Samardzhiska							
Learning the concepts related to Information Security; procedures and methods securing computer systems; methods used to increasing the level of security.11.Course program content: Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptograp Public key cryptography, Hash functions) Cryptographic Algorithms (Types Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryp Schemes) Basic Authentication Terms (Authentication, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication) Basic Authorization Terms (Authorization, Access control matri Authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols with symme cryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Otv Rees, Needham-Schroeder, Public Key Infrastructure) Real Protocols (SSH, SSL / T Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Secu Functions, Trusted OS)12.Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and softv packages), teamwork, case studies, invited guest lecturers, independent preparation defense of a project assignment and seminar work.13.Total available time6 ECTS x 30 hours = 180 hours	9.	Course enrollment prerequisites	Оперативни системи							
Introduction to Information Security (Basic concepts and definitions related to Informa Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptogra Public key cryptography, Hash functions) Cryptographic Algorithms (Types Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryp Schemes) Basic Authentication Terms (Authentication, Authentication meth Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-fa authentication) Basic Authorization Terms (Authorization, Access control matri Authentication models (Multilevel security models, Covert channels, Firewalls, systems) Protocols (Simple protocols, Key exchange protocols with symme cryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Otv Rees, Needham-Schroeder, Public Key Infrastructure) Real Protocols (SSH, SSL / T Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Ty of Malicious Software, Software Attacks) Operating Systems Security (OS Secu Functions, Trusted OS)12.Learning methods: Lectures using presentations, interactive lectures, exercises (using equipment and softw packages), teamwork, case studies, invited guest lecturers, independent preparation defense of a project assignment and seminar work.13.Total available time6 ECTS x 30 hours = 180 hours	10.	Learning the concepts related to Information Security; procedures and methods for								
Lectures using presentations, interactive lectures, exercises (using equipment and softwork packages), teamwork, case studies, invited guest lecturers, independent preparation defense of a project assignment and seminar work.13.Total available time6 ECTS x 30 hours = 180 hours		Introduction to Information Security (Basic concepts and definitions related to Information Security) Basic Cryptographic Terms (Historical examples, Symmetric cryptography, Public key cryptography, Hash functions) Cryptographic Algorithms (Types of Cryptographic Algorithms, Diffie-Hellman Key Exchange, Authentication Encryption Schemes) Basic Authentication Terms (Authentication, Authentication methods, Passwords) Biometric Technologies (Biometrics, Basic concepts and types, Two-factor authentication) Basic Authorization Terms (Authorization, Access control matrices) Authentication models (Multilevel security models, Covert channels, Firewalls, IDS systems) Protocols (Simple protocols, Key exchange protocols with symmetric cryptography, Attacks, Kerberos) Authentication Protocols (Examples with Attacks, Otway- Rees, Needham-Schroeder, Public Key Infrastructure) Real Protocols (SSH, SSL / TLS), Open SSL, Zero-Knowledge Protocols (Fiat-Shamir Protocol) Malicious Software (Types of Malicious Software, Software Attacks) Operating Systems Security (OS Security								
	12.	Lectures using presentations, interactive lectures, exercises (using equipment and software packages), teamwork, case studies, invited guest lecturers, independent preparation and								
14.Distribution of the available time $30 + 45 + 15 + 15 + 75 = 180$ hours	13.	Total available time	6 ECTS x 30 hours = 180 hours							
	14.	Distribution of the available time	30 + 45 + 15 + 15 + 75 = 180 hours							

15.	Teachi	ng acti	ivity f	forms	15.1	. Lectures teaching	30 hour	S			
						. Exercises	(labor seminar pa		, 45 hour	S	
16.	Other activity forms 16.				16.1	. Project Tas	ks		15 hours		
		16.				. Independer Tasks	nt Learning		15 hour	S	
					16.3	. Home learr	ning		75 hour	S	
17.	Assessment methodology										
	17.1. П	ests				10 p			oints		
	17.2. S	.2. Seminar paper/project (presentation: written and oral)						10 points			
	17.3. A	. Activity and learning						10 points			
	17.4. F	7.4. Final exam						70 points			
18.	Assessment criteria (points/grade)				p to 50 points 5 (fiv		ve) (F)				
						51 to 60 poin		6 (six	x) (E)		
						1 to 70 points 7 (seven) (D			ven) (D)		
						1 to 80 points 8 (eight) (C)					
						31 to 90 poin		1	<u>ne) (B)</u>		
10	0		1 4	1 C 1		01 to 100 poi			$\frac{(A)}{(A)}$		
19.	Course require		-	on and final	exam	Realized acti	vittes 15.1	and I	5.2		
20.				P		Macedonian	and English	<u> </u>			
<u>20.</u> 21.		Teaching Language Teaching quality evaluation method				Internal evaluation			mechanisms and		
		• •	-			questionnaires					
22.	Course Material										
	22.1.		-	course material			1				
		No	Author		Title		Publisher		Year		
		1 Mark Stamp			Information		Willey		2011		
				pr pr	securit	•					
					principles and						
			D .		practic		XX7'1		2011		
		2				Computer Wiley Security		2011			
	22.2.	Addit	ional	course material	-						
		No.		Author		Title		Publisher Year			
				1		1					