

1.	Наслов на наставниот предмет	Информациска безбедност Information security
2.	Код	F18L3W043
3.	Студиска програма	Студии за примена на е-технологии, Софтверско инженерство и информациски системи, Компјутерски науки, Компјутерско инженерство, Компјутерска едукација, Интернет, мрежи и безбедност
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатички науки и компјутерско инженерство
5.	Степен (прв, втор, трет циклус)	прв циклус
6.	Академска година / семестар 3 / зимски /	7. Број на ЕКТС кредити 6
8.	Наставник	вонр. проф. д-р Весна Димитрова, доц. д-р Симона Самарциска
9.	Предуслови за запишување на предметот	Оперативни системи
10.	Цели на предметната програма (компетенции): Изучување на поими поврзани со информациската безбедност; постапки и механизми за заштита кај компјутерските системи од безбедносен аспект; методи што се применуваат за подигање на нивото на безбедност во однос на неовластен пристап.	
11.	Содржина на предметната програма: Вовед во информациска безбедност (Основни поими и дефиниции поврзани со информациската безбедност) Основни криптографски поими (Историски примери, симетрична криптографија, криптографија со јавен клуч, хаш функции) Криптографски алгоритми (Видови криптографски алгоритми, Diffie-Hellman размена на клучеви, шеми за автентикациска енкрипција) Основни автентикациски поими (Автентикација, автентикациски методи, лозинки) Биометриски технологии (Биометрика, основни поими и видови, дво-факторска автентикација) Основни авторизациски поими (Авторизација, матрици за контрола на пристап) Автентикациски модели (Повеќенивовски сигурносни модели, прикриени канали, огнени ѕидови, IDS-системи) Протоколи (Едноставни протоколи, протоколи за размена на клучеви со симетрична криптографија, напади, Kerberos) Автентикациски протоколи (Примери со напади, Otway-Rees, Needham-Schroeder, инфраструктура со јавен клуч) Реални протоколи (SSH, SSL/TLS), Open SSL, Zero-knowledge протоколи (Fiat-Shamir протокол) Злонамерен софтвер (Видови злонамерен софтвер, софтверски напади) Безбедност на оперативни системи (Безбедносни функции на ОС, доверливи ОС)	
12.	Методи на учење:	

	Предавања со користење на презентации, интерактивни предавања, вежби (користење на опрема и софтверски пакети), тимска работа, пример случаи, поканети гости предавачи, самостојна изработка и одбрана на проектна задача и семинарска работа.			
13.	Вкупен расположив фонд на време	6 ЕКТС x 30 часа = 180 часа		
14.	Распределба на расположливото време	30 + 45 + 15 + 15 + 75 = 180 часа		
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	30 часови
		15.2.	Вежби (лабораториски, аудиториски), семинари, тимска работа	45 часови
16.	Други форми на активности	16.1.	Проектни задачи	15 часови
		16.2.	Самостојни задачи	15 часови
		16.3.	Домашно учење	75 часови
17.	Начин на оценување			
	17.1.	Тестови	10 бодови	
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)	10 бодови	
	17.3.	Активности и учење	10 бодови	
	17.4.	Завршен испит	70 бодови	
18.	Критериуми за оценување (бодови/ оценка)	до 50 бода		5 (пет) (F)
		од 51 до 60 бода		6 (шест) (E)
		од 61 до 70 бода		7 (седум) (D)
		од 71 до 80 бода		8 (осум) (C)
		од 81 до 90 бода		9 (девет) (B)
		од 91 до 100 бода		10 (десет) (A)
19.	Услов за потпис и полагање на завршен испит	Реализирани активности 15.2 и 16.1		
20.	Јазик на кој се изведува наставата	Македонски и англиски		
21.	Метод на следење на квалитетот на наставата	механизам на интерна евалуација и анкети		
22.	Литература			
	22.1.	Задолжителна литература		

		Ред.бр.	Автор	Наслов	Издавач	Година
		1	Mark Stamp	Information security – principles and practice	Wiley	2011
		2	Dietter Gollman	Computer Security	Wiley	2011
	22.2.	Дополнителна литература				
		Ред. број	Автор	Наслов	Издавач	Година