1.	Наслов на наставниот предмет	Управување со безбедносни инциденти Security incident and response management		
2.	Код	ИТ-И-16		
3.	Студиска програма	Интернет технологии		
4.	Организатор на студиската програма (единица, односно институт, катедра, оддел)	Факултет за информатички науки и компјутерско инженерство		
5.	Степен (прв, втор, трет циклус)	втор циклус		
6.	Академска година / семестар 5 / зимски /	7. Број на ЕКТС кредити 6		
8.	Наставник	вонр. проф. д-р Соња Филипоска, вонр. проф. д-р Анастас Мишев		
9.	Предуслови за запишување на предметот			
10.	Цели на предметната програма (компетенции): Целите на курсот е да му овозможат на студентот да се стекне со знаења поврзани со справување со инциденти поврзани со системската безбедност. Студентот ќе може да разликува настани од инциденти и да ги класифицира инцидентите. Ќе знае да развие полиса за одговор на инциденти. Ќе може да ги истражува мрежните и хост базирани артефакти за да ја одреди главната причина (root cause). Ќе има познавања за алатките и пакетите за поддршка кои се користат во областа.			
11.	Содржина на предметната програма: Дизајн, градење, работа и развој на Computer Emergency Response Team (CERT). Раководење со Security operations center. Одговори на инциденти, планови за одговори на инциденти. Управување со безбедносни настани. Проценка на ранливост, анализа на инциденти. Потреби за полиси. Закони и полиси во употреба. Ограничување на ширењето (containment). Форензика и испитувања. Работа со докази. Работа со форензички тим. Законски одредби за форензика. Управување и комуникација на информацијата. Односи помеѓу тимовите.			
12.	Методи на учење: Предавања поддржани со презентации преку слајдови, интерактивни предавања, практични вежби, тимска работа, пример случаи, поканети предавачи, самостојна изработка на проектна задача и семинарска работа и електронско учење.			
13.	Вкупен расположив фонд на време	6		
14.	Распределба на расположивото време	45 + 15 + 50 + 30 + 40 = 180 часа		
15.	Форми на наставните активности	15.1.	Предавања- теоретска настава	45 часови

		15.2.	Вежби (лабораториски, аудиториски), семинари, тимска работа	15 часови
16.	Други форми на активности	16.1.	Проектни задачи	50 часови
		16.2.	Самостојни задачи	30 часови
		16.3.	Домашно учење	40 часови

17.	Начин на оценување			
	17.1.	Тестови		45 бодови
	17.2.	Семинарска работа/ проект (презентација: писмена и усна)		45 бодови
	17.3.	Активности и учење		10 бодови
	17.4.	Завршен испит		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	
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	Leighton Johnson	Computer Incident Response and Forensic Team Management	Elsevier	2013
2	Jason T. Luttgens, Matthew Pepe, Kevin Mandia	Incident Response & Computer Forensics, Third Edition	McGraw-Hill Education	2014
3	Don Murdoch	GSE Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder	CreateSpace Independent Publishing Platform	2014
4	Tom Olzak	Incident Management and Response Guide: Tools, Techniques, Planning, and Templates	Erudio Security, LLC	2017

22.2. Дополнителна литература

Ред. број	Автор	Наслов	Издавач	Година