1.	**Наслов на наставниот предмет**	**Форензика на мрежи**		
2.	**Код**			
3.	**Студиска програма**	Телекомуникации и информациско инженерство (ТКИИ)		
4.	**Организатор на студиската програма**	Факултет за електротехника и информациски технологии		
5.	**Степен**	Прв циклус на студии		
6.	**Академска година/семестар**	III/6	**7. Број на ЕКТС**	6
8.	**Наставник**	Проф. д-р Александар Ристески		
9.	**Предуслов за запишување на предметот**	Телекомуникациски мрежи		
10.	**Цели на предмететната програма (компетенции)** Запознавање со различни методи на истражување при појава на криминал во комуникациските мрежи. Кандидатите ќе бидат оспособени за Прибирање и анализа на податоци, како и подготовка на извештаи при појава на криминал во комуникациските мрежи.			
11.	**Содржина на програмата** Поим за дигитална форензика и форензиката на мрежи. Дефиницаија на процедура за одговор во случај на инцидент. Методологии за испитување и форензика. Местото на форензиката на мрежи во истражниот процес. Снимање на мрежниот сообраќај во реално време. Пронаоѓање на докази низ мрежата. Прибирање на податоци од сервери и клиенти. Прибирање податоци од мрежни уреди (рутери и комутатори). Дешифрирање на TCP заглавје. Анализа на TCP потпис. Решенија за детекција на упад во мрежа. Форензика на безжични мрежи. Процедура за одговор во случај на инцидент. Вклучување на форензиката на мрежи во процедурата за одговор на случај на инцидент. Скицирање на инфраструктурата на мрежата. Прибирање на постојна документација. Физичка и логичка архитектура на мрежата. Привилегии за пристап до одредени ресурси од мрежата. Запленување на дигитални информации. Дефинирање на дигитален доказ. Методи за запленување на дигитални докази. Избирање на најсоодветна метода за запленување дигитални докази. Преземање активности на самото место на инцидентот. Заштита на опремата и податоците. Запирање на нападот и изолирање на мрежата. Документирање на доказите. Форензика на Интернет-от. Подготовка на извештај и презентирање на резултатите од истрагата. Иднината на дигиталната форензика и форензиката на мрежи.			
12.	**Методи на учење** Интерактивни предавања и вежби, самостојни и групни проекти, домашни задачи, работилници и семинари			
13.	**Вкупен расположив фонд на часови**	180 часови		
14.	**Распределба на расположливото време**	3+1+1+0 45+30+20+15+70 = 180 часа		
15.	**Форми на наставните активности**	15.1. Предавања – теоретска настава		45 часови
		15.2. Вежби, семинари, тимска работа		30 часови
16.	**Други форми на активност**	16.1. Проектни задачи		20 часови
		16.2. Самостојни задачи		15 часови
		16.3. Домашно учење		70 часови
17.	**Начини на оценување**	17.1. Тестови		20 бодови
		17.2. Семинарска работа/проект		15 бодови
		17.3. Активност и учење		5 бодови
		17.4. Завршен испит		60 бодови
18.	**Критериуми за оценување**	до 50 бодови		5 (пет) (F)
		од 51 до 60 бодови		6 (шест) (E)
		од 61 до 70 бодови		7 (седум) (D)
		од 71 до 80 бодови		8 (осум) (C)
		од 81 до 90 бодови		9 (девет) (B)
		од 91 до 100 бодови		10 (десет) (A)
19.	**Услов за потпис и полагање на завршен испит**	Реализирани активности 15.1 и 15.2		
20.	**Јазик на кој се изведува наставата**	Македонски		
21.	**Метод на следење на квалитетот на наставата**	Интерна евалуација и анкети		
22.	**Литература**			

22.1. Задолжителна литература				
Бр.	Автор	Наслов	Издавач	Година
1	Terrence V. Lillard	Digital Forensics for Network, Internet, and Cloud Computing: A Forensic Evidence Guide for Moving Targets and Data	Syngress	
2				
3				
22.2. Дополнителна литература				
Бр.	Автор	Наслов	Издавач	Година
1	Dale Liu	Cisco Router and Switch Forensics: Investigating and Analyzing Malicious Network Activity	Syngress	2009
2	Steven Anson	Mastering Windows Network Forensics and Investigation	Sybex	
3		Интерна скрипта по предметот од предметниот наставник		
4		Статии од стручни и научни списанија		