1.	Наслов на наставниот предмет	Анализа на сајбер закани Cyber threat intelligence
2.	Код	ИТ-И-17
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 / летен /	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): Курсот ќе им овозможи на студентите да се запознаат со фундаменталните концепти и алатки на модерната анализа на сајбер закани. Студентите ќе се здобијат со знаења за животниот циклус на анализата на сајбер закани, идентификацијата, собирањето и интеграцијата на информации за закани и формати на запишување на информацијата.	
11.	Содржина на предметната програма: Разбирање на анализата на закани. Традиционален животен циклус и структурирани аналитички техники. Дефинирање на закани, разбирање на поврзаните ризици. Методи за детекција на закани. Конзумација на информации за закани за различни цели. Градење на тип за анализа на сајбер закани, планирање, насочување, развој на барања и цели. Kill chain модел. Дијамант модел. Извори за собирање информации:: домени, надворешни податочни множества, TLS/SSL сертификати, open source intelligence. Зачувување и структурирање на податоците. Структурирани техники за анализа. Истражување на хипотези. Градење кампањи. Тактичка и оперативна дисеминација. Стандардни технологии за анализа на сајбер закани (пр., CIF сервери, TAXII сервери, SIEM's и други). Откривање на виновникот.	
12.	Методи на учење: Предавања поддржани со презентации преку слајдови, 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, учење во електронско опкружување (форуми, консултации).	
13.	Вкупен расположив фонд на време	6 ECTS x 30 часа = 180 часа
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	Michael Bazzell	Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information	CreateSpace Independent Publishing Platform	2016
2	James Dietle	Effective Threat Intelligence: Building and Running an Intel Team for Your Organization	Amazon Digital Services LLC	2016
3	Florian Skopik	Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level	Auerbach Publications	2017

22.2. Дополнителна литература

Ред. број	Автор	Наслов	Издавач	Година