



Акредитација студијског програма

МАСТЕР АКАДЕМСКЕ СТУДИЈЕ (МАС)

Информациони системи и технологије

Стандард 05. - Курикулум

Табела 5.2 Спецификација предмета

Студијски програм	Информациони системи и технологије				
Назив предмета	01.M20160 Стратегије сајбер безбедности				
Наставник (ци)	Симић Б. Дејан, Редовни професор Јовановић Д. Бојан, Доцент Богићевић Сретеновић С. Марија, Доцент				
Статус предмета	ИМ				
Број ЕСПБ	6				
Услов	Нема.				
Предмети предуслови	Нема				
Циљ предмета	Омогућити студентима разумевање комплексног утицаја и важности примене стратегија сајбер безбедности на организационе циљеве, као и стицање практично употребљивих знања потребних за креирање и имплементацију безбедносних политика, процеса и акција које омогућавају постизање пословних циљева током рада у сајбер простору.				
Исход предмета	Студенти ће добити основна знања неопходна за процену потреба организације у контексту сајбер безбедности. Биће оспособљени да примене стечене вештине за креирање одговарајуће стратегије сајбер безбедности која подржава пословне циљеве и мисију организације.				
Садржај предмета	<p>Теоријска настава</p> <p>П01. Шта је сајбер простор и окружење сајбер простора?. П02. Шта је стратегија и стратегија сајбер безбедности у сајбер простору?. П03. Безбедност у сајбер простору. П04. Управљање комплексним односима у сајбер простору. П05. Стандарди и оквири у области сајбер безбедности и информационе безбедности. П06. <енг<НИСТ</енг> оквир за сајбер безбедност. П07. CIS критичне контроле безбедности . П08. Савремени конфликт у сајбер простору. П09. Алати за сајбер безбедност. П10. Планирање корпоративне политике за сајбер безбедност. П11. Планирање националне политике за сајбер безбедност. П12. Планирање буџета и имплементација. П13. Заштита људских права и приватност личних података. П14.Трендови и правци даљег развоја у области сајбер безбедности. П15. Припрема за испит.</p> <p>Практична настава</p> <p>В01. Анализа инцидената сајбер безбедности. В02. Анализа улога, обавеза и актера у инцидентима везаним за сајбер безбедност. В03. Начини реаговања на сајбер инциденте и могући исходи у односу на актере. В04. Идентификација претњи, ризика и рањивости у контексту сајбер безбедности. В05. Анализа вредности, слабости и кораци у примени стратегија сајбер безбедности. В06. Студија случаја - Phishing напад. В07. Студија случаја - Искоришћавање јавно познате рањивости. В08. Студија случаја - Безбедност мреже. В09. Студија случаја - Инцидент на нивоу апликације. В10. Примена алата за сајбер безбедност. В11. Алати за сајбер безбедност - IP tracker online. В12. Алати за сајбер безбедност - Nmap/Zenmap. В13. Алати за сајбер безбедност - Kali Linux. В14. Алати за сајбер безбедност - Kali Linux. В15. Преглед претходних садржаја и припрема за испит.</p>				
Литература					
Р.бр.	Аутор-и	Наслов	Издавач	Година	
1,	Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short,	Cybersecurity Essentials	Sybex	2018	
2,	William Stallings	Effective Cybersecurity: A Guide to Using Best Practices and Standards	Wiley	2018	
3,	Yuri Diogenes, Erdal Ozkaya	Cybersecurity – Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics	Packt Publishing	2018	
4,	Gregory J. Touhill, C. Joseph Touhill,	Cybersecurity for Executives: A Practical Guide	Wiley	2014	
5,	----	NIST, Framework for Improving Critical Infrastructure Cybersecurity	NIST	2018	
Број часова активне наставе	Теоријска настава	Практична настава			Остали часови
		Вежбе	ДОН	СИР	
	2	2	0	0	0

**Акредитација студијског програма**

МАСТЕР АКАДЕМСКЕ СТУДИЈЕ (МАС)

Информациони системи и технологије

Стандард 05. - Курикулум**Методe извођења наставe****Предавања и вежбе.**

Предавања се изводе по моделу екс катедра, наставник користи обавезно припремљену презентацију коју путем пројектора приказује у учионици. Наставник по потреби користи таблу и маркер за поједине наставне јединице.

Вежбе се изводе у обичној учионици, при чему наставник путем пројектора приказује припремљене презентације као и конкретне алате. Наставник користи таблу и маркер за поједине задатке. Наставник инструкира студенте да подесе потребне алате на сопственим рачунарима и по моделу мешовитог приступа учењу студенти раде на сопственим рачунарима у учионици и код куће.

Практичан рад се одвија по моделу дефинисања пројектног задатка, формирања пројектних тимова и потом њихове израде од стране студената, кроз редовне консултације.

Оцене знања (максимални број поена 100)

Предиспитне обавезе	Обавезна	Поена	Завршни испит	Обавезна	Поена
Активност на предавањима	Да	30.00	Писмени испит	Да	30.00
Пројектни задатак	Да	40.00			