



КЊИГА ПРЕДМЕТА - Информациони системи и технологије

Наставни предмет		Методe заштите у електронском пословању-одабрана поглавља			
Ознака предмета: 01.D20046					
Број ЕСПБ: 10					
Програм(и) у којем се изводи		D02 - Информациони системи и технологије (ДАС), Изборни предмет			
УНО предмета					
Наставници:		Старчевић Б. Душан, Професор Емеритус			
Број часова активне наставе (недељно)					
Предавања	Аудиторне вежбе	Други облици наставе	СИР/СТИР/ИР/ПИР/НИР	Остали часови	
4	0	0	3	0	
Предмети предуслови		Нема			
Услови: Остварена неопходна предзнања на претходним нивоима студија из области заштите рачунарских система.					
1. Образовни циљ:					
Циљ овог предмета је да се студентима омогући стицање знања која се односе на савремене методе заштите у електронском пословању коришћењем научне литературе и најбоље праксе, као и да се студенти оспособе за самосталан истраживачки рад и примену резултата истраживања.					
2. Исходи образовања (Стечена знања):					
Студенти су оспособљени за: 1) свеобухватну анализу резултата истраживања, 2) идентификовање претњи и рањивости, евалуацију постојећих решења и 3) пројектовање и управљање заштитом на основу резултата савремених истраживања у системима електронског пословања.					
3. Садржај/структура предмета:					
Увод. Претње и рањивости савремених система електронског пословања. Модели контроле приступа. Поглавља из криптографије. Примена криптографије у заштити система електронског пословања. Заштита e-mail сервера (PGP, S/MIME). Заштита база података. Заштита Веб апликација. Протоколи за заштиту преноса података (SSL/TLS). Инфраструктура за рад са јавним кључевима (PKI) и децентрализована инфраструктура за рад са јавним кључевима (DPKI). Управљање кључевима и дигиталним сертификатима (X509v3). Квалификовани електронски сертификат и квалификовани електронски потпис. Заштита бежичних мрежа као инфраструктуре у системима електронског пословања. Управљање заштитом у системима електронског пословања. Пример студије случаја – примена PCI DSS и PA DSS стандарда за заштиту трансакција у електронским системима плаћања платним картицама. Примена криптографије у програмском језику Јава. Примена симетричних алгоритама (3-DES, AES). Примена асиметричних алгоритама (RSA). Примена hashing-a (SHA-256, SHA-512). Методе управљања ризиком. Методе провере аутентичности (методе аутентификације). Рад са алатима за заштиту рачунарских мрежа (Wireshark, Metasploit, Nessus и др.). Анализа одабраних стручних и научних радова из области заштите у системима електронског пословања. Студијски истраживачки рад Студијски и истраживачки рад се одвија на основу изабране и додељене научне и стручне литературе.					
4. Методе извођења наставе:					
Настава се одвија у облику предавања или у облику појединачних консултација по наставним јединицама. Истраживачки део обухвата прикупљање и проучавање релевантне литературе са давањем критичког осврта у облику прегледног рада. Практични део обухвата реализацију примера заштите у системима електронског пословања.					
Оцене знања (максимални број поена 100)					
Предиспитне обавезе		Обавезна	Поена	Завршни испит	
Прегледни рад		Да	30.00	Усмени испит	
Рад приређен за публикавање		Да	30.00		
Литература					
Р.бр.	Аутор-и	Наслов		Издавач	Година
1,	William Stallings, Lawrie Brown	Computer Security – Principles and Practice, fourth edition		Pearson Education Limited	2018
2,	William Stallings	Network Security Essentials: Applications and Standards, 6th edition		Pearson Education, Inc.	2016
3,	Kamhoua, Charles A., Njilla, Laurent L., Shetty, Sachin S	Blockchain for Distributed Systems Security		Wiley Blackwell	2019
4,	Naresh Kumar Sehgal, Pramod Chandra P. Bhatt, John M. Acken	Cloud Computing with Security: Concepts and Practices		Springer International Publishing	2020
5,	Dieter Gollmann	"Computer Security", 3rd edition		John Wiley & Sons, Ltd	2011
6,	Joao Manuel R. S.	Handbook of e-business security		Tavares	2019
7,	Jack Caravelli, Nigel Jones	Cyber Security: Threats and Responses for Government and Business		Praeger Security International	2019
8,	Kim Crawley	8 Steps to Better Security: A Simple Cyber Resilience Guide for Business		Wiley	2021