Спецификација предмета за књигу предмета

Студијски програм	Информатика		
Изборно подручје (модул)			
Врста и ниво студија	Докторске академске студије		
Назив предмета	Одабрана поглавља из криптологије		
Наставник (за предавања)			
Наставник/сарадник (за вежбе)			
Наставник/сарадник (за ДОН)			
Број ЕСПБ	12	**Статус предмета (обавезни/изборни)**	изборни
Услов	нема		
Циљ предмета	Стицање теоријских и практичних знања у примени криптографских решења у савременим информационим технологијама. Упознавање са методологијом анализе, синтезе и евалуације напредних крипто система. Упознавање са савременим технологијама за реализацију свеобухватне заштите укључујући: крипто алгоритме гарантованог нивоа сигурности, безбедне носиоце криптографских параметара, и савремене системе за дистрибуцију криптолошких кључева.		
Исход предмета	Знања и вештине неопходне за анализу, синтезу и евалуацију напредних криптосистема, безбедних носиоца криптографских параметара и метода за њихову дистрибуцију. Стичу се знања о примени криптолошких решења у савременим системима електронског пословања електронске управе и професионалних система заштите.		
Садржај предмета			
Теоријска настава	Савремени трендови у развоју криптографских решења, механизама заштите оперативних система и рачунарских мрежама; Криптографска заштита од тачке до тачке; Криптографска заштита од краја до краја у мултитерминалним условима; Методологија синтезе напредних крипто система; Концепт криптолошке синхронизације, Методологија пројектовања генератора псеудослучајних низова (ГПСН); Методологија евалуације ГПСН, Методологија генерисања и дистрибуција криптолошких параметара; Методологија пројектовања синтезе и евалуације криптосистема отпорних на компромитујуће електромагнетно зрачење. Методологија одржавања интегритета криптосистема. Упознавање конкретних страних и домаћих решења заштите. Пројектовање заштите за одабрану реалног система. Овладавање савремном технологијом слојевитог и свеобухватног система заштите.		
Литература			
1	Niels Ferguson, Bruce Schneier and Tadayoshi Koh, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010		
2	Ross Anderson, " Security Engineering", Wiley, 2001		
3	D.R. Stinson, "Cryptograpfy: Theory and Practice", 3Ed, Chapman&Hall/CRC, 2005		
4	N. Ferguson, B.Schneier, "Practical Cryptography ", Wiley, 2003.		

Број часова активне наставе недељно током семестра/триместра/године				
Предавања	**Вежбе**	**ДОН**	**Студијски истраживачки рад**	**Остали часови**
4			2	
Методе извођења	предавања, вежбе, студије случаја, гостујући предавачи			

Оцена знања (максимални број поена 100)			
Предиспитне обавезе	**поена**	**Завршни испит**	**поена**
активност у току	10	**Усмени испит**	50
Истраживачки рад	40		
Укупно	50	Укупно	50