Спецификација предмета за књигу предмета

Студијски програм	Информатика			
Изборно подручје (модул)				
Врста и ниво студија	Докторске академске студије			
Назив предмета	Напредне теме из теорије кодовања			
Наставник (за предавања)				
Наставник/сарадник (за вежбе)				
Наставник/сарадник (за ДОН)				
Број ЕСПБ	11	**Статус предмета (обавезни/изборни)**	изборни	
Услов	нема			
Циљ предмета	Стицање теоријског знања у сагледавању фундаменталних веза између информационих мера неодређености, теорије кодовања, капацитета канала и грешке декодовања са једне стране и показатеља битних у синтези крипто система и система за дистрибуцију шифарских кључева.			
Исход предмета	Студент се оспособљава да на теоријском и практичном нивоу усвоји фундаменталне концепте теорије информација и кодовања и уочи везе са критеријумима битним у анализи и синтези савремених крипто система који по правилу раде у дистрибуираном несигурном информационо-комуникационом окружењу.			
Садржај предмета				
Теоријска настава	Преглед релевантних математичких знања: вероватноћа, теорија информација, теорија комплексности, теорија бројева, теорија кодовањљ, апстрактна алгебра, коначна поља, конвексна оптимизација. Преглед резултата из домена теорије информација битних за напредне крипто системе: Wyner-ов wire-tap канал, Wyner-Ziv-ов поступак кодовања извора са додатном информацијом на страни декодера, Мауреров поступак установљавања тајног кључа јавном дискусијом заснованом на иницијалној заједничкој информацији, Ahlswede-Csiszar-ов капацитет тајности за више терминала, Kannan Ramahandran-ови резултати у домену компресије шифрованих података. Zero-knowledge протоколи; Извлачење приватних информација. Дељење тајни. Shamir-ов метод.			
Литература				
1	Stamp M., Information security: Principles and practice, Hoboken, N.J: Wiley. 2014.			
2	Schneier B., Applied Cryptography: protocols, Algorithms and Source Code in C, Willey, 2015			
3	Stallings, W., Cryptography and network security: Principles and practice. Boston: Pearson, 2017,			

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

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