Спецификација предмета за књигу предмета

Студијски програм	Електротехника и рачунарство		
Изборно подручје (модул)	Рачунарство и информатика		
Врста и ниво студија	Основне академске студије		
Назив предмета	Заштита информација		
Наставник (за предавања)	Вучковић В. Владан		
Наставник/сарадник (за вежбе)	Рајковић Ј. Петар		
Наставник/сарадник (за ДОН)	Рајковић Ј. Петар		
Број ЕСПБ	5	**Статус предмета (обавезни/изборни)**	Изборни
Услов			
Циљ предмета	Овладавање основним знањима неопходним за употребу основних и напредних поступака у заштити информација.		
Исход предмета	Теоријска знања: Овладавање математичким техникама за кодирање и декодирање података; Програмирање метода заштите информација на рачунару.		
Садржај предмета			
Теоријска настава	Елементи криптологије, криптографије и криптоанализе. Ауторизовани приступ. Методе идентификације. Развој система са ауторизованим приступом. Симетрична криптографија. Јавни и тајни кључ. Hash функције. Метода напада на заштићени систем. Сертификати, одржавање и издавање сертификата. Основни сигурносни протоколи. Типови malware програма.		
Практична настава (вежбе, ДОН, студијски истражива-чки рад)	Израда семинарских радова. Историјски преглед области и имплементација најједноставнијих алгоритма кодирања. Општа анализа кодера, токова података и имплементација алгоритама A5, A5/1 и RC-4. Фајстелов кодер. Имплементација кодера блокова података DES, TDES, AES, TEA. Модови кодера. Асиметрично кодирање, имплементација алгоритама RSA и Knapsack. Рачунање CRC вредности. Tiger-hash. Анализа и имплементација MD и SHA фамилија криптографских хеш–функција. Методе за криптоанализу.		
Литература			
1	Mark Stamp, “Information Security Principles and Practice“, John Wiley and Sons, Inc, New Jersey, U.S.A., 2006.		
2	Владан Вучковић, Петар Рајковић “Заштита информација” основни уџбеник, Електронски факултет Ниш, 2016, прво издање. 195 стр, ISBN 978-86-6125-166-5, COBISS.SR-ID 226243852.		
3	Владан Вучковић, Петар Рајковић “Заштита информација”, Едиција: помоћни уджбеник, Електронски факултет, Ниш , 2010. , ISBN 978-86-6125-010-1		
4			
5			

Број часова активне наставе недељно током семестра/триместра/године				
Предавања	**Вежбе**	**ДОН**	**Студијски истраживачки рад**	**Остали часови**
2	2	1	0	0
Методе извођења наставе	Предавања, вежбе на табли, лабораторијске вежбе, самосталан рад студената на изради домаћих задатака и пројеката, консултације.			

Оцена знања (максимални број поена 100)			
Предиспитне обавезе	**поена**	**Завршни испит**	**поена**
активност у току предавања		**писмени испит**	
практична настава	20	**усмени испит**	40
колоквијуми	30		
семинари	10		