

## Спецификација предмета за књигу предмета

<b>Студијски програм</b>		Рачунарство и информатика		
<b>Изборно подручје (модул)</b>		Безбедност рачунарских система		
<b>Врста и ниво студија</b>		Мастер академске студије		
<b>Назив предмета</b>		Пројектовање и имплементација сигурног софтвера		
<b>Наставник (за предавања)</b>		Јанковић С. Драган		
<b>Наставник/сарадник (за вежбе)</b>		Рајковић Ј. Петар		
<b>Наставник/сарадник (за ДОН)</b>				
<b>Број ЕСПБ</b>		<b>4</b>	<b>Статус предмета (обавезни/изборни)</b>	Изборни
<b>Услов</b>				
<b>Циљ предмета</b>	Циљ предмета је упознавање студената са основним концептима и примењеним техникама за развој програмског кода повећане сигурности			
<b>Исход предмета</b>	Након одслушаног курса студенти треба да буду у стању да препознају основне проблеме везане за сигурност софтверских решења и примене научене технике за њихово отклањање			
<b>Садржај предмета</b>				
<b>Теоријска настава</b>	1. Увод 2. Лозинке 3. Псеудослучајни бројеви 4. Генератори псеудослучајних бројева 5. Buffer Overflow 6. Механизми за повећање безбедности 7. Проблем закључавања дељивих ресурса 8. Валидација улаза 9. Криптографија 10. Протоколи за аутентикацију 11. Конфигурабилност софтвера 12. Рад са осетљивим подацима 13. Рад са меморијом			
<b>Практична настава (вежбе, ДОН, студијски истраживачки рад)</b>	1. Слаба места у шел скриптовима 2. Криптовање лозинки 3. Апликације које се базирају на псеудослучајним бројевима 4. Имплементација рандом генератора 5. Методе за превазилажење Buffer Overflow проблема 6. Имплементација матрица за контролу приступа 7. Начини за спречавање закључавања програмских нити 8. Начини за спречавање закључавања фајлова 9. Валидација улазних података 10. Употреба протокола за аутентикацију 11. Примена криптографских алгоритама у софтверу 12. Креирање и коришћење конфигурација 13. Алоцирање и деалоцирање меморије			
<b>Литература</b>				
	1 Anderson, Ross. Security engineering. John Wiley & Sons, 2008.			
	2 Richardson, Theodor, and Charles N. Thies. Secure software design. Jones & Bartlett Publishers, 2012.			
	3 Michael Howard, David LeBlanc: Writing Secure Code, ISBN 073561722-8, Microsoft Press, 2002.			
	4 Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security, Private Communication in a Public World, Prentice-Hall, 2002.			
	5 Fernandez-Buglioni, Eduardo. Security patterns in practice: designing secure architectures using software patterns. John Wiley & Sons, 2013.			
<b>Број часова активне наставе недељно током семестра/триместра/године</b>				
<b>Предавања</b>	<b>Вежбе</b>	<b>ДОН</b>	<b>Студијски истраживачки рад</b>	<b>Остали часови</b>
2	1	0		
<b>Методе извођења наставе</b>	предавања, аудиторне и лабораторијске вежбе			
<b>Оцена знања (максимални број поена 100)</b>				
<b>Предиспитне обавезе</b>	<b>поена</b>	<b>Завршни испит</b>		<b>поена</b>
активност у току предавања	5	писмени испит		30
практична настава	15	усмени испит		20
колоквијуми				
семинари	30			