Програм предмета

Студијски програм	ФИТ4, ФИТ3		
Изборно подручје (модул)			
Врста и ниво студија	Основне академске		
Назив предмета	Заштита информација		
Наставник (за предавања)	Др Ђорђе Бабић, доцент		
Наставник/сарадник (за вежбе)	Мр Драго Видовић, виши асистент		
Шифра предмета	ФИТ-3230		
Број ЕСПБ	7	**Статус предмета (обавезни/изборни)**	Обавезни
Услов	Нема		
Циљ предмета	Стицање општих знања из области заштите у рацунарслим мрежама и PKI (Public Key Infrastructure) система.		
Исход предмета	По завршетку курса, студент има основна знања о системима и технологијама заштите савремених рацунарских мрежа, као што су дигитални потпис, шифровање и PKI системи. Упознат је са принципима вишеслојне архитектуре заштите рацунарских мрежа, као и са основама примене smart картица и хардверских безбедносних модула. Такође, свестан је неопходности израде политика безбедности у оквиру информационог система организације. Може да развије базицне криптографске функције за потребе дигиталног потписа и шифровања, као и да успостави основни PKI систем.		
Садржај предмета			
Теоријска настава	Оцењивање и третирање безбедносних ризика. Политика безбедности. Физичка безбедност. Трендови у заштити рачунарских мрежа. Потенцијални напади. Могући начини одбране. Технологије заштите. Стандардни криптографски алгоритми (симетрични DES, IDEA, асиметрични RSA). Дигитални потпис. Дигитална енвелопа. PKCS стандарди. Вишеслојна аритектура заштите. Заштита на апликационом нивоу. S/MIME протокол. Заштита Web трансакција. Токени, смарт картице и биометрика. Заштита на транспортном нивоу. SSH, SSL, TLS, WTLS протоколи. Заштита на мрежном нивоу. IPSec. Аутентикациони протоколи удаљеног приступа. PPTP и L2TP протоколи. VPN. Kerberos. Firewall уредаји. Вишеструка firewall архитектура. Сигурност бежицних 802.x мрежа. Смарт картице. HSM уредаји. Софтверска и хардверска решења заштите. PKI системи. Дигитални сертификати. Компоненте PKI система. CA. RA.		
Практична настава (вежбе, ДОН, студијски истраживачки рад)	*** вјежбе обухватају рјешавање конкретних проблема,		
Литература			
1	Д. Плескоњић, Н. Мачек, Б. Ђорђевић, М. Царић Сигурност рачунарских система и мрежа Микро књига 2007		
2			
3			
4			
5			

Број часова активне наставе недељно током семестра/триместра/године

Предавања	Вежбе	ДОН	Студијски истраживачки рад	Остали часови
3	3			

Методе извођења наставе	• Теоретску наставу, • Аудиторне вежбе, • Групно учешће студената на пројекту, или израду семинарских радова и мини пројеката (према потребама и интересовању студената), • Одржавање консултација са студентима,

Оцена знања (максимални број поена 100)

Предиспитне обавезе	поена	Завршни испит	поена
активност у току предавања	10	писмени испит	30
практична настава	30	усмени испит	
колоквијуми	20		
семинари	10		