

Студијски програм: Софтверско инжењерство			
Назив предмета: Информациона безбедност			
Наставник: Драган Ђ. Солеша, Ликавец Љ. Силвиа			
Статус предмета: Изборни			
Број ЕСПБ: 7			
Услов: Упис			
Циљ предмета Оспособљавање студената за примену метода и техника за моделовање и успостављање информационе безбедности у оквиру различитих система. Упознавање студената са основним концептима заштите података. Разумевање основа криптографије и сигурносних протокола.			
Исход предмета Студенти су у стању да примене принципе, методе и стандарде у области информационе безбедности. Оспособљени су да реализују управљање информационом безбедношћу, управљању безбедносним ризицима и успостављање информационе безбедности у различитим организацијама. Студенти ће стећи знања о начинима за одвраћање, детекцију, спречавање и неутралисање нарушавања сигурности.			
Садржај предмета <i>Теоријска настава</i> Увод у информациону безбедност: дефиниција основни појмови, развој информационе безбедности. Потреба за дефинисањем информационе безбедности: претње на безбедност информација, напади на информациони систем, пословни, професионални и етички разлози за дефинисање информационе безбедности, законски оквири. Стандарди у информационој безбедности. One-Time-Pad, Алгоритми тока (RC4), блоковски алгоритми (DES, AES), асиметрични алгоритми (DiffieHellman, RSA), хеш функције (MD-5, SHA). Лозинке, шифрирање лозинки, шифрирање симетричним кључевима, покушаји декриптовања шифре са симетричним кључевима, стандарди за дигитално шифрирање, токени, биометрички уређаји, проблеми са дистрибуирањем јавних кључева, шифрирање несиметричним кључем, PKI инфраструктура, дигитални потпис, мрежни и транспортни сигуросни протоколи, сигурносни протоколи на нивоу апликација, хардверска решења за шифрирање. <i>Практична настава:</i> Вежбе, Други облици наставе, Студијски истраживачки рад Симулација шифрирања и дешифрирања, праћење мрежног саобраћаја, сигурносни пренос информација. Апликације за аутентикацију (Kerberos, X.509). Заштита електронске поште (PGP, S/MIME). Заштита у рачунарским мрежама (IP Security). Заштита на интернету (SSL).			
Литература <i>Основна</i> Михаљевић, М.(2022). Информациона безбедност и блокчејн технологија (Том 48, стр. 43 стр.). САНУ. Вулетић, П., Станисављевић, Ж. (2025). Заштита података. Универзитет, Електротехнички факултет; Академска мисао.. Raković, R. (2017). Bezbednost informacija: osnove i smernice. Akademska misao. <i>Додатна</i> Stallings, W. (2023). Computer Security: Principles and Practice (5th ed.). Pearson. Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security			
Број часова активне наставе	Теоријска настава: 2x15=30	Практична настава: 2x15=30	
Методе извођења наставе Предавања, вежбе у информатичкој лабораторији, рад на пројектима, семинарски радови и дискусије у online окружењу			
Оцена знања (максимални б број поена 100)			
Предиспитне обавезе	поена	Завршни испит	Поена
активност у току предавања	10	писмени испит	50
практична настава	10	усмени испит	
колоквијум-и	20		
семинар-и	10		