

Спецификација предмета за књигу предмета

| | | | | |
|--|---|--|-----------------------------------|----------------------|
| Студијски програм | | Рачунарство и информатика | | |
| Изборно подручје (модул) | | Безбедност рачунарских система | | |
| Врста и ниво студија | | Мастер академске студије | | |
| Назив предмета | | Безбедност рачунарских мрежа | | |
| Наставник (за предавања) | | Миловановић И. Емина, Ћирић М. Владимир | | |
| Наставник/сарадник (за вежбе) | | Димитријевић М. Александар | | |
| Наставник/сарадник (за ДОН) | | | | |
| Број ЕСПБ | | 4 Статус предмета (обавезни/изборни) | | Изборни |
| Услов | Рачунарске мреже | | | |
| Циљ предмета | Циљ предмета је да студенти стекну увид у потенцијалне безбедносне слабости мрежа и добију основна знања за повећање безбедности, као и потребна апликативна знања и вештине које могу применити у циљу повећања безбедности рачунарских мрежа. | | | |
| Исход предмета | Очекује се да студент може да сагледа безбедносне аспекте мреже и планира стратегије за повећање безбедности. Такође се очекује да студент може да примени алате за повећање безбедности и имплементира безбедносне протоколе на мрежи. | | | |
| Садржај предмета | | | | |
| Теоријска настава | Циљеви безбедности: заштита података, интегритет података, аутентификација. Криптографски алгоритми: заштита јавним и дељеним кључем. Механизми размене кључева. Дигитални потпис. Безбедносни аспекти на различитим мрежним слојевима, протоколи и механизми за заштиту од конкретних типова напада. Безбедносни протоколи за заштиту података, заштиту интегритета података и аутентификацију (Kerberos, SSL/TLS, IPSec, VPN, PK, PGP, S/MIME). Примена firewall алата у заштити система. Напади. Рачунарски вируси. Безбедност бежичних рачунарских мрежа. | | | |
| Практична настава (вежбе, ДОН, студијски истраживачки рад) | Рад на примерима кроз сет лабораторијских вежби. Заштита мрежне опреме. Имплементација криптографских алгоритама. Имплементација безбедносних протокола на мрежном, транспортном и апликативном нивоу. Имплементација SSL/TLS и SSH протокола. RADIUS и AAA сервери. Firewall. Конфигурација виртуалних приватних мрежа (VPN). Заштита бежичних мрежа. Типични напади. | | | |
| Литература | | | | |
| | 1 | William Stallings, Osнове bezbednosti mreža, prevod 5. izdanja, CET, 2014. | | |
| | 2 | William Stallings, "Cryptography and Network Security: Principles and Practice (5th Edition)", Prentice hall, 2011 | | |
| | 3 | Michael Watkins, Kevin Wallace, "CCNA Security", Cisco Press, 2008, ISBN 9781587202209 | | |
| | 4 | | | |
| | 5 | | | |
| Број часова активне наставе недељно током семестра/триместра/године | | | | |
| Предавања | Вежбе | ДОН | Студијски истраживачки рад | Остали часови |
| 2 | 1 | 0 | | |
| Методје извођења наставе | Предавања, вежбе на табли, лаб вежбе. | | | |
| Оцена знања (максимални број поена 100) | | | | |
| Предиспитне обавезе | поена | Завршни испит | | поена |
| активност у току предавања | 10 | писмени испит | | |
| практична настава | | усмени испит | | 50 |
| колоквијуми | 20 | | | |
| семинари | 20 | | | |