

Табела 5.2. Спецификација предмета

Студијски програм: ССС Процена безбедносних ризика			
Назив предмета: Процена безбедносних ризика у ИКТ системима			
Наставник/наставници: Мирјана Мисита, Ненад Путник			
Статус предмета: изборни			
Број ЕСПБ: 6			
Услов: нема			
Циљ предмета			
Циљ предмета је да слушалац буде оспособљен да идентификује, препозна, процени безбедносне ризике у ИКТ системима као и да примени стандарде серије ИСО 27000 о систему менаџмента безбедношћу информација, и примени опште уредбе о заштити података.			
Исход предмета			
Слушалац је по завршетку курса способан да препозна/описе и разуме појам безбедности информација, разуме документовани систем менаџмента безбедношћу информација ИСМС. његово успостављање, имплементацију, примену, праћење, преиспитивање, одржавање. Након одслушаног курса студент је способан да анализира постојећи ИСМС и предложи побољшања ИСМС-а. Такође студент је оспособљен за примену опште уредбе о заштити података ГДПР.			
Садржај предмета			
<i>Теоријска настава</i>			
Основни појмови, регулаторна тела. надлежни органи. Тело за координацију послова информационе безбедности. Превенција и заштита од безбедносних ризика у ИКТ системима (Национални ЦЕРТ, посебни ЦЕРТ-ови, ЦЕРТ-ови републичких органа). Потреба за информационом безбедношћу. Документовани ИСМС – Систем Менаџмента Безбедношћу. Стандард ИСО 27000. Успостављање ИСМС, имплементација ИСМС, примену ИСМС, праћење ИСМС, преиспитивање ИСМС, одржавање ИСМС и побољшавање ИСМС. Опште уредбе о заштити података (General Data Protection Regulation – скраћено ГДПР. Начела ГДПР. ГДПР - правни, технички и организациони аспект заштите података. Обука за ГДПР.			
<i>Практична настава</i>			
Студенти самостално, за дати практични пример организације разматрају пословник о безбедности информација, процедуре и записе, разматрају успостављање имплементацију, примену и праћење ИСМС-а. Пројектни задатак се односи на процену ефикасности посматраног ИСМС-а, анализи одржавања ИСМС-а и предлагању о побољшања посматраног ИСМС-а.			
Литература			
1. ISO/IEC 27000:2016 - серија стандарда			
2. Закон о заштити података о личности, "Службени гласник РС", број 87/2018.			
3. Закон о критичној инфраструктури, "Службени гласник РС", број 87/ 2018.			
4. Закон о информационој безбедности, "Службени гласник РС", број 6/2016 и 94/2017.			
5. Путник, Н. (2018). Систем корпоративне безбедности: информациони аспекти. У: Кековић, З., Димитријевић, И., Шекарић, Н. (прир.), <i>Корпоративна безбедност - хрестоматија</i> . (стр. 53-75). Београд: Универзитет у Београду - Факултет безбедности.			
6. Мандић, Г., Путник, Н., Милошевић, М. (2017). Заштита података и социјални инжењеринг - правни, организациони и безбедносни аспекти. Београд: Универзитет у Београду - Факултет безбедности.			
Број часова активне наставе:	Теоријска настава: 45	Практична настава: 30	
Методe извођења наставе			
Предавања, аудиторне важбе, лабораторијске.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе	поена	Завршни испит	поена
активност у току предавања	-	писмени испит	70
практична настава	10	усмени испит	
колоквијум-и	20	
семинар-и	-		