Табела 5.2. Спецификација предмета

Студијски програм: Обука службеника (менаџера) за заштиту података о личности
Назив предмета: Информационе технологије и заштита података о личности
Наставник/наставници: Ненад Путник, предавач са стране
Статус предмета: Обавезни
Број ЕСПБ: 5
Услов:
Циљ предмета Циљ предмета је да студенте упозна са безбедносним и техничко-технолошким аспектима процеса прикупљања, обраде, чувања и заштите података о личности. Садржај предмета је осмишљен тако да студентима пружи свестран увид у разноврсне, сложене и међусобно повезане безбедносне ризике и претње усмерене ка информационо-комуникационим технологијама (ИКТ) и подацима који се, посредством ових технологија, обрађују, размењују и чувају. Осим тога, циљ предмета је и да студенте упозна са међународним и домаћим стандардима у области информационе безбедности и добром праксом на пољу заштите информационих система и података о личности у дигиталном облику.
Исход предмета Изучавање предмета за свој иход има сагледавање безбедносне и техничко-технолошке димензије процеса прикупљања, обраде, чувања и заштите података о личности и овладавање практичним знањима и вештинама неопходним за процену ризика у рачунарским системима, као и за осмишљавање политике безбедности информација (принципа, правила и процедура) и примену савремених техничко-технолошких решења на пољу њихове заштите.
Садржај предмета *Теоријска настава* У оквиру теоријске наставе студенти изучавају следеће садржаје: појам информационих технологија; појам информационе и сајбер безбедности; појам критичне инфраструктуре и критичне информационе инфраструктуре; појам, етиологија и феноменологија безбедносних претњи у сајбер простору; регулаторна тела и 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); процена ризика у рачунарским системима; балансирање улагања у безбедност на смањење ризика; информациона безбедност као део политике пословања; однос безбедности ИКТ са менаџментом и осталим областима управљања ризиком; потреба за увођењем стандарда, правила, упутстава и процедура; израда корпоративне политике информационе безбедности и стратегије заштите од безбедносних претњи у сајбер простору; документовани систем менаџмента безбедношћу (ISMS); стандарди серије ИСО/ИЕЦ 27000:2015; улога технологије и иновација у заштити података о личности; нове технологије и заштита приватности. *Практична настава* Студије случаја – студенти самостално, за задати модел организације разматрају корпоративну политику информационе безбедности и примењене физичке, техничке и логичке мере заштите информационих система и осетљивих података. Пројектни задатак се односи на процену ефикасности задатог интегралног система безбедности, анализу адекватности политике информационе безбедности, одржавања система менаџмента безбедношћу и предлагању потенцијалних побољшања у циљу унапређења заштите података о личности. Радионице – разматрање улоге савремених ИКТ у заштити података о личности и дискусије о негативним ефектима технолошког развоја на заштиту приватности. Упознавање са новим технологијама и техничким решењима у вези заштите података о личности.
Литература Обавезна Путник, Н. (2018). Систем корпоративне безбедности: информациони аспекти. У: Кековић, З., Димитријевић, И., Шекарић, Н. (прир.), *Корпоративна безбедност – хрестоматија*. (стр. 53-75). Београд: Универзитет у Београду – Факултет безбедности Мандић, Г., Путник, Н., Милошевић, М. (2017). *Заштита података и социјални инжењеринг – правни,*

организациони и безбедносни аспекти. Београд: Универзитет у Београду – Факултет безбедности

Милошевић, М., Путник, Н. (2017). Сајбер безбедност и заштита од високотехнолошког криминала у Републици Србији – стратешки и правни оквир, *Култура полиса*, год. XIV, бр. 33, стр. 177-191

Путник, Н., Милошевић, М. (2016). Смернице за израду политике безбедности информационо-комуникационих ресурса и њихових корисника у образовно-васпитном систему. У: Поповић Ћитић, Б., Липовац, М. (уредници), *Безбедност у образовно-васпитним установама: основна начела, принципи, протоколи, процедуре и средства* (стр. 97-116). Београд: Факултет безбедности

Закон о критичној инфраструктури, "Службени гласник РС", број 87/ 2018

Закон о информационој безбедности, "Службени гласник РС", број 6/2016 и 94/2017

ISO/IEC 27000:2016 – серија стандарда

Data protection. European Commission – European Commission.

Privacy notices under the EU General Data Protection Regulation ico.org.uk.

Допунска

Димитријевић, И., Путник, Н., Кучековић, З. (2018). Мониторинг друштвених мрежа као облик надзора у образовно-васпитним установама. У: Липовац, М., Станаревић, С., Кешетовић, Ж. (Ур), *Безбедност у образовно-васпитним установама и видео-надзор*. (стр. 127-144). Београд: Универзитет у Београду – Факултет безбедности

Број часова активне наставе	**Теоријска настава:**	**Практична настава:**

Методе извођења наставе

Предавања, вежбе, колоквијум, радионице и семинари.

Оцена знања (максимални број поена 100)

Предиспитне обавезе	поена	**Завршни испит**	поена
активност у току предавања		писмени испит	
практична настава		усмени испт	
колоквијум-и		.....	
семинар-и			

Начин провере знања могу бити различити наведено у табели су само неке опције: (писмени испити, усмени испт, презентација пројекта, семинари итд.....