

Табела 5.2. Спецификација предмета

Студијски програм : Примењена математика (МАП)			
Назив предмета: ЗАШТИТА ПОДАТАКА (П603)			
Наставник/наставници: Ивана Војновић			
Статус предмета: обавезни на модулу Аналитика података и статистика			
Број ЕСПБ: 5			
Услов:			
Циљ предмета Циљ предмета је упознавање студената са математичким као и практичним, системским, методама за заштиту података и база података.			
Исход предмета Студент је упознат са значајем и основним математичким и системским методама, као и практичним системима, за заштиту података. На тај начин, уз додатно упознавање са регулативама и сличним аспектима (на пример GDPR) студент је оспособљен да, при развоју апликација и алгоритама за аналитику података, узме у обзир и ефективно примени заштиту података.			
Садржај предмета <i>Теоријска настава</i> Различити принципи и методе за унапређење приватности и тајности података: агрегација, анонимизација, аутентификација, ауторизација, основе криптографије: симетрична енкрипција, интегритет порука, public key енкрипција. <i>Практична настава</i> Упознавање са примерима практичних система и платформи за заштиту података и њиховог начина функционисања.			
Литература 1. J. Katz and Y. Lindell, Introduction to Modern Cryptography - Principles and Protocols , Taylor and Francis, 2008. 2. Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications , John Wiley & Sons, 2010. 3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of applied cryptography , CRC Press, 1996.			
Број часова активне наставе		Теоријска настава: 2	Практична настава: 2
Методe извођења наставе Предавања; понављање; активно учешће студената у решавању проблема. Тестови знања–домаћи задаци. Демонстрација функционалности реалних система за заштиту података.			
Оцена знања (максимални број поена 100)			
Предиспитне обавезе	поена	Завршни испит	поена
Домаћи задаци, мини пројекат	30	Завршни испит	70