

<b>Студијски програм :</b> ОАС Примењена математика			
<b>Назив предмета:</b> Заштита података (26.П141)			
<b>Наставник/наставници:</b> Давор Кумозец, Бојан Башић			
<b>Статус предмета:</b> обавезни на модулу Аналитика података и статистика			
<b>Број ЕСПБ:</b> 5			
<b>Услов:</b> нема			
<b>Циљ предмета</b> Циљ предмета је упознавање студената са математичким као и практичним, системским, методама за заштиту података и база података.			
<b>Исход предмета</b> 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.			
<b>Садржај предмета</b> <i>Теоријска настава</i> Различити принципи и методе за унапређење приватности и тајности података: агрегација, анонимизација, аутентификација, ауторизација, основе криптографије: симетрична енкрипција, интегритет порука, <i>public key</i> енкрипција. <i>Практична настава</i> Упознавање са примерима практичних система и платформи за заштиту података и њиховог начина функционисања.			
<b>Литература</b> 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.			
<b>Број часова</b>	<b>активне наставе</b>	<b>Теоријска настава:</b> 2	<b>Практична настава:</b> 2
<b>Методe извођења наставе</b> Предавања; понављање; активно учешће студената у решавању проблема. Тестови знања–домаћи задаци. Демонстрација функционалности реалних система за заштиту података.			
<b>Оцена знања (максимални број поена 100)</b>			
<b>Предиспитне обавезе</b>	поена	<b>Завршни испит</b>	поена
Домаћи задаци, мини пројекат	30	Завршни испит	70