

Наставна дисциплина	Безбедност и заштита на компјутерско-комуникациони системи				
Семестар	Вид	Фонд на часови	Кредити	Јазик	Институт
X	изборен	2+0+2+2	5	МК	КТИ
Предуслови					
Компетенции*	Продлабочени познавања од полето на безбедност и заштита на компјутерските и мрежните околии. Примена на стекнатите познавања во практични системи во делот на компјутерски системи и мрежи од сите можни типови. Заштита на банкарски и криптични податоци.				
Содржина	<p>Вовед и основни поими. Етички норми и одговорност. Структура на криптирање. Примери на протоколи за криптирање. Криптирање со тајни клучеви. Криптирање со јавни клучеви. Пробивање на криптирани системи. Основни заштитни механизми кај оперативните системи. Архитектура на системите за заштита кај оперативни системи, автентикација, контрола на пристаплисти на пристап, имплементација на контрола на пристап (Unix, Java), Bell и La Padula модели, Механизми на оперативни системи за подршка на MAC политиките, Безбедносни политики Clark-Wilson и Кинески сид. Слабости на заштитата кај оперативните системи. Безбедни јадра на опер. Системи. Заштитни механизми кај TCP/IP базираните мрежи и кај DNS. Заштитни сидови (Firewalls). Детекција на вируси, тројански коњи и обиди за неовластено најавување. Spam (преку e-mail подсистем). Агенти и мобилни кодови. Заштита кај smart и други видови на картички. Протоколи за безбедни електронски трансакции. Студентски проекти.</p> <p>Литература:</p> <ol style="list-style-type: none"> 1. Dieter Gollman, Computer Security, John Wiley & Sons, 1998 2. Shifting the Odds: Writing (More) Secure Software, Steve Bellovin, AT&T research, 1996 3. B. Schneier, Applied Cryptography Second Edition: protocols, algorithms, and source code in C, John Wiley & Sons, 1996 4. Jan Harrington, An Introduction to Network Security, Morgan Kaufmann Publishers Inc., September 2004 				