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*	По завршувањето на курсот се очекува студентот да има продлабочени познавања од полето на безбедност и заштита на компјутерските и мрежните околини. Примена на стекнатите познавања во практични ситеми во делот на компјутерски системи и мрежи од сите можни типови. Заштита на банкарски и критични податоци.				
Содржина	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 пристап:листи 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 ѕид. Слабости на заштитата кај оперативните системи. Безбедни јадра на опер. Системи. Заштитни механизми кај TCP/IP базираните мрежи и кај DNS. Заштитни ѕидови (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. Литература: 1. M. Whitman, H. Mattord, Principles of Information Security, Thomson Course Technology, 2009. 2. B. Graham, D. Dodd, Security Analysis, 6th Edition, McGraw-Hill, 2009 3. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition, Wiley Publishing, 2008				