Сигурност на компјутерски системи (3+2) 6 ECTS

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; Безбедност во комуникациските програми *Microsoft Explorer* и *Netscape Communicator*. Безбедност во бази податоци. Безбедност на Јава и скрипт јазици. Безбедност во оперативните системи: *UNIX, NT, Novell*.

Предуслови: Оперативни системи

Литература: Dietter Gollman, Computer Security, John Wiley & Sons, 1998, B. Schneier, Applied Cryptography Second Edition: protocols, algorithms, and source code in C, John Wiley & Sons, 1996, Jan Harrington, An Introduction to Network Security, Morgan Kaufmann Publishers Inc., September 2004