# Информациска безбедност/ Безбедност на компјутерски системи

## Вовед во курсот

Проф. д-р Весна Димитрова

# Предавачи

- Фонд на часови
  - 2+1+2 (6 кредити)
- Предавања
  - Д-р Весна Димитрова
- Теориски и лабораториски вежби
  - Д-р Христина Михајлоска-Трпческа

# Литература


- 1. Mark Stamp: **Information security – principles and practice**, John Willey and Sons,
- 2. Dietter Gollman: **Computer Security**, John Wiley & Sons,
- 3. Bruce Schneier: **Applied Cryptography Second Edition: protocols, algorithms, and source code in C**, John Wiley & Sons,
- 4. William Stalings: **Cryptography and network security – Principles and practice**, Prentice hall,
- 5. Jan Harrington: **An Introduction to Network Security**, Morgan Kaufmann Publishers Inc.,
- 6. William Stalings: **Network security**, Prentice hall.

# Сајтови

- Moodle ecourses
- Сите известувања ќе ги имате на сајтот

# Содржина на курсот

- Цел на предметната програма:
  - Изучување на поими поврзани со информацискатa безбедност;
  - постапки и механизми за заштита кај компјутерските системи од безбедносен аспект;
  - методи што се применуваат за подигање на нивото на безбедност во однос на неовластен пристап.

# Содржина на курсот

- Вовед во информациска безбедност
  - Основни поими и дефиниции поврзани со информацискатa безбедност
- Основни криптографски поими
  - Историски примери, симетрична криптографија, криптографија со јавен клуч, хаш функции
- Криптографски алгоритми
  - Видови криптографски алгоритми, Diffie-Hellman размена на клучеви, шеми за автентикациска енкрипција
- Основни автентикациски поими
  - Автентикација, автентикациски методи, лозинки, Биометриски технологии (Биометрика, основни поими и видови, дво-факторска автентикација)
- Основни авторизациски поими
  - Авторизација, матрици за контрола на пристап

# Содржина на курсот

- Автентикациски модели
  - Повеќенивовски сигурносни модели, прикриени канали, огнени ѕидови, IDS-системи
- Протоколи
  - Едноставни протоколи, протоколи за размена на клучеви со симетрична криптографија, напади, Kerberos
- Автентикациски протоколи
  - Примери со напади, Otway-Rees, Needham-Schroeder, инфраструктура со јавен клуч
- Реални протоколи
  - SSH, SSL/TLS, Open SSL, Zero-knowledge протоколи (Fiat-Shamir протокол)
- Злонамерен софтвер
  - Видови злонамерен софтвер, софтверски напади
- Безбедност на оперативни системи
  - Безбедносни функции на ОС, доверливи ОС

# Вреднување – оценка

- Крајната **оценка** на студентот ќе зависи од реализацијата на следниве 3 дела. За секој дел е даден процентот кој е вклучен во вкупната оцена.
  - Тест – прашања и задачи (60 поени)
  - Лабораториски вежби – мин. презентација на една вежба (10 поени)
  - Проект – мах. 3 студенти (30 поени)
  - Дополнителна активност (+10 поени)
- За положување е потребно да имате 50 поени од вкупните поени.

Ви посакуваме успешна работа!