FIŞA DISCIPLINEI

Universitatea Academiei de Ştiinţe a Moldovei **Facultatea Ştiinţe exacte**	**Denumirea cursului:** Securitatea informaţiei **Codul cursului în planul de studii:** S.06.A.045
Nivelul calificării ISCED: 6 **Domeniul de formare profesională:** 444 Informatică **Specialitatea :** 444.1 Informatică	**Catedra responsabilă de curs:** Matematică şi Informatică **Titular/Responsabil de curs:** Izbaş Vladimir, dr. conf. univ.

Total ore			Număr de ore pe tipuri de activităţi			Forma de evaluare	Număr de credite
total	contact direct	studiu individual	curs	seminar	laborator		
120	**42**	**78**	**14**	**0**	**28**	**E**	**4**

Descrierea succintă a corelării cursului cu programul de studii

Cursul de lecţii *Securitatea Informaţiei* este predestinat studenţilor ciclului I (universitar) şi are ca scop pregătirea matematică a studenţilor la nivelul necesar şi suficient pentru soluţionarea unor probleme teoretice şi practice legate de securitate. Conţinutul disciplinei oferă cunoştinţele necesare pentru ca viitorii specialişti să poată lua măsuri de securitate absolut necesare în orice companie. Securitatea informaţiei este obţinută prin implementarea unui set adecvat de politici, practici, proceduri, structuri organizaţionale şi funcţii software. Aceste elemente trebuie implementate în măsura în care se asigură atingerea obiectivelor specifice de securitate. Prezentarea cursului se realizează prin expunere orală cu demonstraţii ale aplicaţiilor la calculator. Studenţilor li se oferă cunoştinţe despre noţiunile de bază ale criptografiei: criptare, sistem de criptare, aritmetică modulară, cifruri bloc, criptoanaliză, Hash funcţii, semnătură electronică. La seminare studenţii sunt antrenaţi în aplicarea cunoştinţelor la cazuri concrete, cât şi la demonstrarea unor rezultate suplimentare. Activităţile individuale ale studentului sunt orientate spre aprofundarea cunoştinţelor dobândite, aplicaţiile lor în matematici industriale, teoria algoritmilor, criptografie, care sunt expuse în formă scrisă.

Competenţe dezvoltate în cadrul cursului

Competenţe generale:

- capacitatea de a aplica cunoştinţele teoretice la studiul problemelor practice;
- programarea în limbaje de nivel înalt;
- dezvoltarea şi întreţinerea aplicaţiilor informatice;
- utilizarea instrumentelor informatice în context interdisciplinar;
- utilizarea bazelor teoretice ale informaticii şi a modelelor formale;
- proiectarea şi gestiunea bazelor de date;
- proiectarea şi administrarea reţelelor de calculatoare;
- capacitatea de a lucra atât independent, cât şi în echipă, în funcţie de cerinţele activităţii profesionale.

Competenţe specifice:

- Cunoașterea și aplicarea rețelelor de calcul, a soft-ului de sistem in activități de studiu și cercetare;
- dezvoltarea capacității de memorare, generalizare și analiză critică a informației, care permite viitorului specialist să se adapteze operativ la modificările din societate;
- aplicarea metodologiei contemporane de cercetare in soluționarea problemelor cu caracter interdisciplinar;
- identificarea direcţiilor prioritare de cercetare in domeniul informaticii;
- argumentarea importanței investigațiilor privind diverse modele ale matematicii aplicate și a softului instrumental, cu potențial de utilizare in soluționarea problemelor de automatizare a gestiunii activităților;
- dezvoltarea capacității de administrare a rețelelor de calculatoare, a sistemelor de operare a bazelor de date din cadrul unităților economice;
- utilizarea cunoștințelor obținute în activități de proiectare a sistemelor suport inteligente, aplicațiilor pentru dispozitive mobile, diverse sisteme de simulare, diverse aplicații în rețea etc., în scopul îmbunătățirii calității vieții;
- diseminarea informației și a cunoștințelor dobândite atât specialiștilor din domeniu, cât și celor din alte domenii.

Finalităţi de studii ale cursului

La nivel de aplicare studenţii vor:

- analiza unele exemple importante, aplica teoria generală în aceste cazuri;

- considera algoritmi specifici criptografiei clasice şi cu chei publice, atât cu scop ilustrativ (în activitatea de laborator), cât şi ca exerciţii de proiectare (proiecte individuale);
- prezenta metode de criptare şi elemente de criptanaliză.

La nivel de integrare studenţii vor:

- utiliza metodele criptografice în alte domenii sau cu alte scopuri: noţiuni fundamentale legate de redundanţa semnalelor (limbaj natural, imagini), codarea imaginilor, algoritmi complecşi;
- extinde şi aplica metodele criptografice în alte domenii;
- identifica exemple de utilizare a unor teoreme celebre din teoria numerelor în unele aplicaţii pentru criptografie;
- dezvolta abilităţi de a proiecta noi sisteme de cifrare eficiente;
- disemina cunoştinţele dobândite specialiştilor din alte domenii.

Condiţii prerechizit: pentru studierea cursului *Securitatea Informaţiei* sunt necesare cunoştinţe iniţiale în Teoria numerelor, Teoria structurilor algebrice, Teoria probabilităţilor, Logica matematică,teoria grafurilor, Reţele de calculatoare, Algoritmi şi programare, Baze de date.

Teme de bază: Noţiuni de bază. Securitate informaţională. Criptografie. Criptologie. Cifruri de substituţie. Sisteme de criptare monoalfabetice şi polialfabetice. Fundamente matematice ale criptografiei. Aritmetica modulară. Noţiuni de teoria informaţiei şi probabilitate. Sistemul de criptare DES şi cifruri bloc. Sisteme de criptare cu chei publice. Sistemul RSA. Criptosistemul El Gamal. Funcţii de dispersie (Hash funcţii).Algoritmi şi scheme de semnătură electronică (digitală). Sisteme de semnătură digitală pe bază de logaritmare discretă.

Strategii de predare-învăţare: prelegeri, lucrări individuale, consultaţii.

Strategii de evaluare: teste de evaluare, prezentări, rapoarte, dezbateri, elaborarea portofoliilor, teze/proiecte etc. Nota finală se constituie din rezultatul evaluării finale (40%), curente (40 %) şi calităţii lucrului individual al studentului pe parcursul semestrului (20%).

Bibliografie selectivă:

1. Adrian Atanasiu, *Curs de criptografie. http://www.galaxyng.com/adrian_atanasiu/cript.htm*
2. *A.* Salomaa, *Criptografie cu chei publice*, Bucureşti, Ed. Militară, 1994
3. D. Stinton, Cryptography, *Theory and Practice*, Chapman & Hall/CRC, 2002
4. A. Menezes, P. Oorschot, S. Vanstome, *Handbook of Applied Cryptography,*1997
5. A.Schneier, - *Applied Cryptography*, John Wiley & Sons, second edition, 1997
6. Н. Смарт, *Криптография Москва*: Теосфера, 2005. -528 с.
7. С. Коутинхо, *Введение в теорию чисел. Алгоритм RSA*. Москва: Постмаркет, 200.-328 с.
8. В.О.Осипян, К. В. Осипян, *Криптография в упражнениях и задачах*. Москва: «Гелиос АРВ», 2004
9. Buşneag D., Boboc F., Piciu D., *Aritmetica şi teoria numerelor*, Editura Universitară, Craiova, 1999

Data

Semnătura